Guide

Intel® vPro™ Technology

Intel® Active Management Technology Deployment and Reference Guide

Version 1.0

October 2006

315610-001US

Intel Active Management Technology requires the platform to have an Intel AMT-enabled chipset, network hardware and software, connection with a power source and a network connection.

Intel Virtualization Technology requires a computer system with an enabled Intel processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain platform software enabled for it. Functionality, performance or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

Table of Contents

Section 3 – continued

Section 4 – continued

Appendix A – continued

Appendix B – continued

TABLES

FIGURES

Introduction

Welcome to the deployment and reference guide for Intel® Active Management Technology (Intel® AMT). This guide provides simple, step-by-step processes for setting up and configuring the Intel AMT capabilities in PCs with Intel® vPro™ technology.

Because networking and security are complex areas that often require significant expertise, this guide also includes reference information about security methods and technologies, enterprise network configurations and requirements, and configuration management. In addition, this guide offers general information on deployment planning, POC evaluations and pilot tests, information on Intel AMT, and common uses of Intel AMT features that can help you get started taking advantage of the new hardware-based capabilities.

This guide includes these sections:

- **Section 1: Quick Start,** which provides step-by-step procedures for setting up and configuring Intel AMT.
- **Section 2: Overview of Intel AMT,** which briefly describes the hardware-based Intel AMT capabilities.
- **Section 3: Security Methods and Technologies,** which describes reference information about the security technologies, methodologies, and techniques used to protect the powerful, out-of-band capabilities built into PCs with Intel AMT.
- **Section 4: Setup and Configuration,** which provides detailed reference information on network requirements, common MEBx (Intel® Management Engine BIOS extension) parameters, process variations, and other information useful for setting up and configuring Intel AMT in an enterprise environment in both static and dynamic IP environments.
- **Section 5: Configuration Management,** which provides information about changing configurations, and erasing and reestablishing setup information for Intel AMT.
- **Appendix A: Best known methods,** for establishing a stable, secure management environment for Intel AMT-enabled PCs.

Note:
To help IT administrators who might not be as experienced in establishing such an environment, this guide provides detailed background information on security, setup, and configuration for PCs with Intel AMT.

- **Appendix B: Use Cases,** to help you identify processes where Intel AMT can help deliver service improvements, and provide a starting point for a POC evaluation or pilot study.
- **Appendix C: Deployment Planning,** to help you assess the value of Intel AMT for your business environment.
- **Appendix D: Glossary and Acronyms.**

Audience

Deployment of PCs with Intel AMT requires technical skills and knowledge of enterprise networking, security methods and technologies, application programming interfaces (APIs), and provisioning processes for large networks.

This document is intended for authorized IT administrators who are experienced in:

- System administration
- Security methodologies and technologies, including Transport Layer Security (TLS), secure sockets layer (SSL), and preshared key infrastructures (PKI)
- IT management tools and consoles

This document is not intended for IT administrators who serve small- or medium-business (SMB) networking environments. Security, which is critical aspect of setup and configuration for Intel vPro technology, is usually established through a different infrastructure in SMB environments than in enterprise environments. If you are an IT administrator in the SMB environment, refer to the appropriate SMB administrator's guide for information about setting up and deploying Intel AMT in SMB sites.

Scope

This guide explains how to set up and configure Intel AMT in an enterprise environment in which dynamic host configuration protocol (DHCP) and domain name servers (DNS) are available. This document also explains how to deploy PCs with Intel AMT in static IP mode for enterprise environments in which DHCP and/or DNS are not available, or are not being used for security reasons.

In addition, this guide includes information about Intel AMT and some common ways to use the Intel AMT features. However, this document does not explain Intel AMT or Intel vPro technology in detail. For detailed information about Intel vPro technology or Intel AMT, refer to the Intel Web site, or contact your local Intel sales representative.

Virtualization capabilities

For information about setting up and configuring virtualization capabilities for your environment, refer to the Intel vPro technology deployment guide for Intel® Virtualization Technology (Intel® VT).

This guide also explains general processes for deployment planning, including mapping business needs to usage models and planning a POC evaluation. For detailed information on setting up POC evaluations, pilot tests, and case studies, contact your local Intel account team. To use the return-on-investment estimator for Intel AMT to investigate some of the potential benefits of Intel AMT in your environment, visit the Intel Web site.

Terminology

A few common terms are used with specific meanings throughout this guide:

- **PC** – a PC with Intel AMT.
- **Configuration service** – a third-party configuration application that loads Intel AMT with configuration information, including Kerberos settings, access control lists, and settings that activate Intel AMT.
- **MEBx** – the Intel Management Engine BIOS extension, through which the Intel AMT network and security settings are configured.
- **OS** – the operating system on the PC with Intel AMT. Also called the host.

Additional terms and acronyms used in this guide are listed or described in an appendix at the end of this guide.

For more information

Network configuration and security are complex areas where significant knowledge is often required in order to ensure a stable, well-secured environment. To help IT administrators who might not be as experienced in establishing such an environment, this guide provides detailed background information on security, setup, and configuration for PCs with Intel AMT.

In addition, Intel offers training in best known methods (BKM) for deploying systems to an enterprise environment. Intel can also provide a list of authorized dealers and channel service providers who are experienced in deploying PCs with Intel AMT. For information about training, contact your Intel account team or local sales office.

Case studies, evaluation reports, and white papers about POC tests and pilot studies in customer environments can be found on the Intel Web site. Contact your Intel account team or local sales office for help in setting up your own POC evaluation.

Section 1
Quick Start

Introduction

Welcome to the deployment and reference guide for Intel® Active Management Technology (Intel® AMT).

Setting up and configuring Intel AMT capabilities is relatively simple. Most steps are actually performed automatically by Intel AMT or by your configuration service (CS). Once the initial security information for Intel AMT is set up, automated configuration typically takes only a few seconds.

This quick-start section briefly explains the procedures for setting up and configuring Intel AMT in enterprise environments using dynamic IP or static IP networking:

- Automated setup using a USB storage device
- Manual setup for dynamic IP networking
- Manual setup for static IP networking
- OEM factory setup
- Automated configuration in a dynamic IP or static IP environment
- Manual configuration in a static IP environment

Recommended: In-house setup

In environments in which security is a high-priority, Intel recommends that you establish the bootstrap security credentials for PCs in-house, rather than use OEM-supplied security credentials.

Reference information available

To help IT administrators who might not be as experienced in establishing a stable, well-secured environment, this guide also provides background and reference information and best practices on security, setup, and configuration for PCs with Intel AMT. Additional procedures for post-deployment configuration management are provided later in this guide.

Intel AMT and the PC

Intel AMT is one aspect of Intel® vPro™ technology. Specifically, Intel AMT is part of the powerful Intel Management Engine of Intel vPro technology.

Terminology

- CS – configuration service
- MEBx – the management engine BIOS extension
- OEM – original equipment manufacturer
- PID – provisioning ID
- PPS – provisioning passphrase
- PSK – preshared key

Note

The setup and configuration processes described in this guide are not for the PC in general or for Intel vPro technology, but for Intel AMT.

CS not typically available during setup

In a typical deployment, the configuration service (CS) is not available to Intel AMT until after the PCs have been moved to their working location and are ready for configuration.

* Other names and brands may be claimed as the property of others.

TLS-PSK setup considerations

During setup, keep these considerations in mind:

- The digitally signed image is not changed.
- Customization is to the data area only.
- Passwords and PID-PPS pairs should be kept confidential.

Deployment requirements

Table 1-1 lists the network deployment requirements for enterprise operation in dynamic and static IP environments.

Table 1-1. Setup and configuration requirements

Network element	Dynamic IP	Static IP
DHCP service	Required	–
DNS service	Required	Optional[1]
Certificate authority service	Required	Required
Configuration service	Required	Required
Support for Microsoft Active Directory*	Optional[1]	Optional[1]

[1] If you choose to use Kerberos security, you will need an environment that supports Microsoft Active Directory.

These procedures assume that the typically required enterprise network services and applications are available.

Deployment process

The deployment process follows four general steps:

1. Establish the management console, including the configuration service.
2. Generate unique key pairs for each PC.
3. Set up Intel AMT with security credentials for networking and TLS.
4. Configure Intel AMT with power policies, Kerberos settings, access control lists, certificates and keys, and the settings that activate Intel AMT.

Figure 1-1 shows the general process for deploying PCs with Intel AMT.

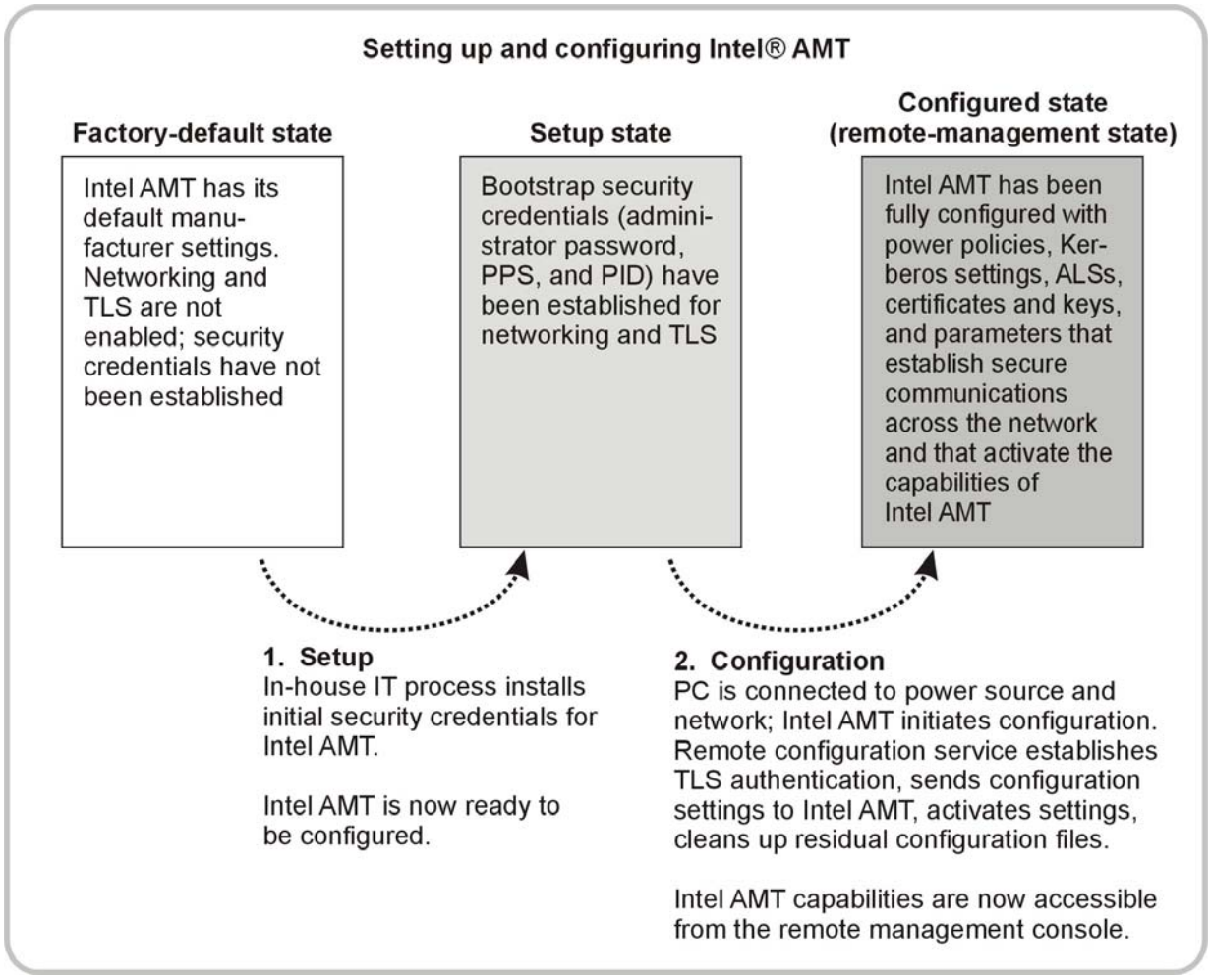

Figure 1-1. Setup and configuration states. Intel AMT is set up and configured so that the powerful remote-management capabilities are available to authorized IT technicians.

Additional information

Background and reference information on setup and configuration considerations, methodologies, and settings is provided in the setup and configuration section.

Deployment considerations

Keep the following brief considerations in mind as you set up and configure Intel AMT.

Factory-default settings for BIOS and MEBx

Your hardware vendor should have set several BIOS and MEBx settings to default values appropriate for your network. Table 1-2 lists the typical default settings and the values of those settings after setup.

Terminology

- CA – certificate authority
- DHCP – dynamic host configuration protocol
- DNS – domain name server
- Dynamic IP – DHCP

Default settings

The Intel Management Engine and Intel AMT are usually disabled by default. For more detailed information about enabling the management engine and Intel AMT, refer to the setup and configuration section of this guide.

Table 1-2. BIOS and MEBx settings

BIOS or MEBx setting	Typical default	Value after setup
Intel® Management Engine	Disabled	Enabled[1]
Sleep-state power policies for Intel Management Engine	Off for S1 – S5	On for S1 – S5[2]
Intel AMT	Disabled	Enabled[1]
Provisioning mode	Enterprise	Enterprise
TLS	Enabled	Enabled
DHCP	Enabled	Enabled for dynamic IP networking Disabled for static IP networking

[1] The Intel Management Engine and Intel AMT must be enabled in order for you to set up, configure, and use Intel AMT.

[2] Setting power policies for the management engine to S1 - S5 allows Intel AMT to initiate configuration in any power state, as soon as the PC is connected to power and plugged into the network.

Changing usernames and passwords

Note the following considerations when changing the factory-default username and password.

- Enter correct admin username. The username-password pair for each PC is provided by your OEM.
- Do not assume the username-password pair. Verify the username-password pair as per the OEM documentation for the PC.
- Change the username, not just the password.

Additional information on username-password considerations is provided in the setup and configuration section of this guide.

Setup procedures

This discussion provides setup procedures for Intel AMT in different environments, automatically and manually. These procedures assume that the default BIOS and MEBx parameters are set as described in Table 1-2, earlier in this section.

Setup: Automated setup using a USB-key storage device

In this procedure, a USB storage device is used to automatically install the administrator password, PPS, and PID for the Intel AMT capabilities. The USB device interprets and parses changes of the default password, PPS, and PID. The procedure described here assumes that BIOS and MEBx parameters are set to the typical default values described in Table 1-2, earlier in this section.

Setup is the same for both dynamic IP and static IP environments.

Follow these steps to enter setup information automatically in each PC via a USB storage device:

1. Using your third-party configuration service, request that the service generate a provisioning passphrase (PPS) and a provisioning ID (PID).

   The configuration service should then generate a TLS premaster secret and store the premaster secret in a database, along with other setup and configuration information (such as operational mode, TLS setting, and so on).

   The configuration service also stores the PPS, PID, new administrator password, and other configuration data in your USB storage device.

2. Remove the PC from its box and connect the PC to a power source using the power cable.

3. Plug the USB storage device into the PC.

4. Power up the PC.

   As BIOS loads, it loads BIOS and MEBx settings, including enabling the Intel Management Engine, setting power policies for management-engine sleep states, and enabling Intel AMT. BIOS then reads the new BIOS administrator password, PPS, and PID, as well as other required information from the USB storage device.

   When BIOS has finished reading the settings from the USB device, the BIOS will continue the boot process and finish loading.

   Caution

   Do not power down the PC during this process. The BIOS must be allowed to finish loading in order to activate the settings and complete the setup process.

Setting up the CS

For information about how to use the CS, refer to your third-party documentation or the appropriate setup and installation guide for your CS or manage-ability solution.

Recommended defaults

The PC manufacturer specifies the BIOS settings for Intel AMT. However, Intel recommends that the default settings are enterprise mode, TLS enabled, and dynamic IP.

Establishing certificates

An experienced IT administrator can set up an isolated staging environment to fully set up and configure Intel AMT before PCs are delivered to the user desk. This can be useful in environments in which security is a high priority.

Caution

Do not power down or otherwise interrupt the PC during the setup process. Each PC's unique ID is associated with the specific USB key used to provision that PC. If the setup process is interrupted, you may have to manually reset that PPS and PID. At worst, the interruption might have voided a PPS-PID pair in the PSK repository, and may prevent the PC associated with that PPS-PID pair from authenticating the configuration service (as well as any remote management server) that attempts to communicate with the system.

5. Power down the PC.
6. Remove the USB storage device.

The PC is now ready to be sent to the user and go through the self-initiated automated Intel AMT configuration, as described later in this guide.

Setup: Manual setup for dynamic IP networks

This procedure explains how to set up Intel AMT by manually entering security credentials. Credentials are specified through the MEBx (management engine BIOS extension) screens. This procedure assumes that BIOS and MEBx parameters are set to the typical default values described in Table 1-2, earlier in this section.

1. Using your third-party CS, request that the CS generate a provisioning passphrase (PPS) and a provisioning ID (PID). The CS should generate a TLS premaster secret and store the secret in a database, along with other information (such as operational mode, TLS setting, and so on). The CS then provides you with a copy of the PPS and PID.
2. Remove the PC from its box, connect the PC to a power source, and power up the system.
3. In BIOS, make sure the Intel Management Engine is enabled throughout the BIOS.
4. Using the appropriate keyboard function key (as defined by the PC manufacturer), display the MEBx configuration screen.

   Depending on the BIOS, you should be prompted to log into MEBx when you access the MEBx configuration screen.
5. Log into the MEBx using the factory-default admin username and password. The default username and password are provided in the manual or shipping box for the PC.

   Because this is the first login to the device, the system will require that you change the default administrator password.
6. Change both the administrator username and password, as described in the best-practices appendix in this guide.
7. Using MEBx features, make sure the manageability mode is set to Intel AMT.
8. Using the MEBx power-control feature, verify that the Intel AMT power policies for sleep states are set to your operational preference.
9. In the MEBx screen, now select the PID and PPS option.
10. Enter the PPS and PID for the system.
11. Exit the MEBx screen. The BIOS will then continue to load.

Caution

Do not power down the PC during this process. The BIOS must be allowed to finish loading in order to activate the settings and complete the setup process.

Typical defaults

The PC manufacturer specifies the BIOS settings for Intel AMT. Typically, the default settings are enterprise mode, TLS enabled, and dynamic IP.

Change username, not just password

When working with localized BIOS, the authentication process requires that you change only the default password. However, best practices suggest that you also change the administrator username from the factory default to something more unique.

Establishing certificates

An experienced IT administrator can set up an isolated staging environment to fully set up and configure Intel AMT before PCs are delivered to the user desk. This can be useful in environments in which security is a high priority.

Caution

Do not power down or otherwise interrupt the PC during the setup process. Each PC's unique ID is associated with the specific USB key used to provision that PC. If the setup process is interrupted, you may have to manually reset that PPS and PID. At worst, the interruption might have voided a PPS-PID pair in the PSK repository, and may prevent the PC associated with that PPS-PID pair from authenticating the configuration service (as well as any remote management server) that attempts to communicate with the system.

12. Power down the PC.

The system is now ready to be installed at the user desk and perform its self-initiated, automated configuration.

Default settings

The Intel Management Engine and Intel AMT are usually enabled by default, so that you can access the MEBx.

Establishing certificates

An experienced IT administrator can set up an isolated staging environment to fully set up and configure Intel AMT before PCs are delivered to the user desk. This can be useful in environments in which security is a high priority.

Change username, not just password

When working with localized BIOS, the authentication process requires that you change only the default password. However, best practices suggest that you also change the administrator username from the factory default to something more unique.

Disabling networking

If you choose to disable networking, the TCP/IP settings are automatically reset to disable DHCP, and the IP address of the configuration server is set to 0.0.0.0.

Setup: Manual setup for static IP networks

This discussion explains how to set up Intel AMT for static IP. In this setup procedure, you will manually entering security credentials and change the DHCP, DNS, and IP address settings for the system. This procedure assumes that BIOS and MEBx parameters are set to the typical default values described in Table 1-2, earlier in this section.

Follow these steps to set up Intel AMT using typical MEBx options:

1. Using your third-party CS, request that the service generate a provisioning passphrase (PPS) and a provisioning ID (PID).

   The CS should generate a TLS premaster secret. The CS should then store the premaster secret in a database, along with other information (such as operational mode, TLS setting, and so on). The CS then provides you with a copy of the PPS and PID.

2. Remove the PC from its box, connect the PC to a power source, and power up the system.
3. In BIOS, make sure the Intel Management Engine is enabled throughout the BIOS.
4. Using the appropriate keyboard function key (as defined by the OEM), display the MEBx configuration screen. The BIOS will then prompt you to log in.
5. Log into MEBx using the factory-default administrator username and password. Because this is the first login to the device, the system will require that you change the default administrator password.
6. Change both the administrator username and password.
7. Using MEBx features, make sure the manageability mode is set to Intel AMT.
8. Using the MEBx power-control feature, verify that the Intel AMT power policies for sleep states are set to your operational preference.
9. Using MEBx features, specify the name of the PC's operating system (the host). The host name is the name assigned to the PC's operating system for identification purposes.
10. Now select the TCP/IP option.
11. Make sure networking capabilities remain enabled.
12. Disable DHCP. This will allow you to manually specify the IP address for Intel AMT.

DHCP not available

In static IP environments, you must usually manually disable DHCP, enter the DNS domain name, and enter the IP addresses for Intel AMT and the DNS server.

DHCP and DNS not available

If both DHCP and DNS are not available, you must manually disable DHCP, then enter the IP address for both Intel AMT and the configuration server.

DNS not really optional

The DNS field is technically an optional field. However, you must supply this value if you want the PC to automatically query the DNS to locate the IP address of the configuration service.

Specifying a DNS address

If you want to specify a DNS address, you must use the same name that will be used by the PC's operating system (the host). That name is used in the TLS certificate and is required for successful handshaking and authentication.

13. Enter the TCP/IP settings as appropriate for your static IP service environment:
    - IP address for Intel AMT. The host name is the name assigned to the PC's operating system for identification purposes. This must be different from the IP address that will be specified for the PC's operating system.
    - Subnet mask
    - Default gateway address
14. If Intel AMT will be using DNS to resolve the IP address, also enter DNS information and optionally, the domain name:
    - Preferred DNS address
    - Alternate DNS address (optional)
    - Domain name (optional)
15. Using MEBx features, enter the PPS and PID for the system.
16. Verify that the provisioning model is set to enterprise provisioning.
17. Exit MEBx. The BIOS will then continue to load.

Caution

Do not power down the PC during this process. BIOS must be allowed to finish loading in order to activate the settings and complete the setup process.

18. Power down the PC.

The system is now ready to be installed at the user desk and perform its self-initiated, automated Intel AMT configuration.

Power state for management engine

If your OEM has shipped your PCs with the Intel Management Engine off for Sx (sleep states 1 through 5), the user might need to power up the PC later, at the user desk, in order to activate the management engine. Intel AMT will then be able to initiate its automated configuration.

TLS-PSK setup and security considerations

If the PC vendor sets up Intel AMT for you, keep these considerations in mind:

- The digitally signed image is not changed.
- Customization is to the data area only.
- Passwords and PID-PPS pairs should be kept confidential.
- For security reasons, you should replace OEM-defined passwords and PID-PPS pairs during in-house configuration of the Intel AMT capabilities of these PCs.

Setup: Factory setup

In environments in which security is a high-priority concern, Intel recommends that initial security credentials for Intel AMT be established in-house. However, your OEM may choose to set up the default administrator password, PPS, and PID for you, as part of their service. The procedure described here assumes that BIOS and MEBx parameters are set to the typical default values described in Table 1-2, earlier in this section.

The hardware vendor will typically use a factory firmware image tool or an ICT (in-circuit test) tool to generate and configure PID and PPS values into a flash device. The tool keeps a database of values (UUID, MACs, PID, PPS) that are burned into the flash device.

Factory-automated setup, which loads the initial security credentials into Intel AMT for networking and TLS, follows several general steps:

1. The OEM enables the Intel Management Engine throughout BIOS, sets the power policies for the management engine, and enables Intel AMT in MEBx.
2. A factory firmware image tool (or ICT tool) generates and configures PID and PPS values into the Intel AMT nonvolatile memory.
3. The OEM loads the PC's universal unique identifier (UUID) and MAC(s) into the Intel AMT nonvolatile memory. The OEM may also choose to customize other setup parameters during this procedure.
4. At the end of a production run (or at appropriate intervals), the tool uploads its database of values onto a CD/DVD-ROM.
5. The factory ships the CD/DVD-ROM to the enterprise IT department.
6. The IT department loads the database from the CD/DVD-ROM into the configuration server being used to configure Intel AMT.

Because the system has now been set up with the appropriate keys and certificates, the system is ready to go through its automatic configuration. For PCs whose Intel AMT capabilities are already set up, the systems can be delivered directly to the user desk. Once the user connects the PC to a power source and plugs the system into the network, Intel AMT will initiate and complete its own configuration process.

No need to manually power up the PC

PCs with Intel AMT are enabled for out-of-band communication. They do not necessarily have to be powered up in order to establish a connection to the configuration server, or to perform the self-initiated and automatic configuration process. Upon the customer request, the PC manufacturer can ship the system with the Intel Management Engine on for first application of power.

Ping PCs even before they're configured

A remote management console can discover an Intel AMT-enabled PC even before it has been configured, by pinging the IP address in the clear. Secure discovery and management of PCs should be done after systems are configured and security certificates established.

Configuration: Automated procedure

Once Intel AMT is set up and in its working location (such as at the user desk), it is ready for automated configuration. Configuration assumes that the configuration service is available on the network.

The automated enterprise configuration process is the same for both dynamic and static IP environments. The procedure requires only one step:

1. Connect the PC to a power source and the network.

Intel AMT automatically initiates its own configuration process by trying to locate the configuration server using DHCP and DNS, or via the static IP settings specified during setup. Once the PC and configuration service (CS) establish secure communications, the CS loads the settings and data required for your environment. The CS completes the process by rebooting the PC.

Caution

Do not interrupt the PC during the configuration process. Security certificates – which include a time and date stamp – are established during configuration. Interrupting this process could result in invalid security certificates and prevent successful configuration.

When configuration is complete, Intel AMT is in its fully configured state, and the capabilities are ready for use in the enterprise environment.

Validation

PCs with Intel AMT basically validate themselves when they complete their automated configuration process.

Validating that Intel AMT is properly enabled

For PCs with Intel AMT, successful completion of the configuration process is also validation that the Intel AMT capabilities, security, and networking have been set up properly. This is because, during configuration, security certificates are built and transported, the management console and Intel AMT are resolved to the same management domain, the management engine is communicating properly, Intel AMT is up and running, and the Intel AMT Web server is working properly. Configuration cannot complete unless the security and network settings have been properly established.

Confirmation that configuration has completed successfully should be stored in the configuration log managed by your configuration service or management console.

Once Intel AMT is successfully configured, the management console can update its database with the address of the new PC. This typically occurs on an automated schedule, at intervals of usually 4 to 24 hours. Once the PC has been added to the management domain, you can manually (or automatically) validate that Intel AMT capabilities are accessible from the management console by performing a remote-management task unique to Intel AMT. For example, you could upload the unique ID, hardware asset information, BIOS settings, or other persistent information from the Intel AMT nonvolatile memory.

Refer to the documentation for your third-party management console for information about automating validation of communication with the Intel AMT capabilities.

Successful configuration is also validation

Successful completion of the configuration process (which uses the SOAP API to communicate with Intel AMT), validates that networking, security, and the Intel AMT capabilities are properly configured.

Validating that security is properly established

In environments in which security is a high priority, Intel does not recommend that the Web graphical user interface (GUI) be enabled in order to validate that the security credentials have been properly set up for Intel AMT.

However, an experienced IT administrator could use the Web GUI to validate security. Typically, the IT administrator would set up the configuration service to perform these steps:

1. Enable the Web GUI.
2. Establish an HTTP-S session to communicate with the Intel AMT-enabled PC, using the secure port 16993.
3. Communicate with Intel AMT. For example, the configuration service could upload the PC's unique ID, hardware asset information, or BIOS version number to confirm communication.
4. Disable the Web GUI.

Such a process could specifically validate secure communications for Intel AMT.

Terminology

The unconfiguring and reconfiguring processes are also sometimes called "unprovisioning" and "provisioning."

Returning to factory-default state

Refer to the configuration-management section in this guide for information about unconfiguring and reconfiguring Intel AMT, and returning Intel AMT to its factory-default settings.

For more information

The next several sections of this guide provide information about security methodologies and techniques, networking requirements, and setup and configuration parameters. This guide also provides a general overview of Intel AMT capabilities, use cases, and deployment information and processes.

For additional information about Intel AMT, refer to the Intel Web site.

Section 2
Overview of Intel® Active Management Technology

Introduction

Intel AMT allows information technology (IT) administrators to perform many remote tasks for their networked computing assets, regardless of PC power state or the state of the OS. This includes the ability to remotely inventory, monitor, maintain and update, boot, troubleshoot, repair, rebuild, and remediate systems. The hardware-based capabilities of Intel AMT are delivered to IT organizations through third-party management and security applications.

The advantage of the hardware-based capabilities of Intel AMT over traditional software-based solutions is in allowing remote access to PCs that have traditionally been unavailable to the management console. PCs with Intel AMT deliver management and security capabilities even when powered off, if the OS is inoperative, or if software agents are missing. This out-of-band communication helps IT organizations streamline remote services, automate more tasks, and achieve a new level of service across the network

This section introduces Intel AMT, which is designed to help IT organizations:

- Improve security of PCs, even for a PC's power is off, its OS is inoperative, or its management agent is disabled.
- Improve compliance with government and other regulations.
- Reduce deskside visits for both software and hardware problems.
- Improve the effectiveness of remote diagnostics and repair, even if the OS is locked-up or hardware (such as a hard drive) has failed.
- Increase the accuracy of inventories and software licensing.
- Reduce total cost of ownership (TCO) of technology.

PCs with Intel AMT already enjoy widespread industry support. For copies of white papers, technology evaluations, and other

Intel® AMT

Intel® Active Management Technology (Intel® AMT) is one aspect of the new hardware-based capabilities of Intel® vPro™ technology

Intel® Virtualization Technology

PCs with Intel vPro technology also include the robust, hardware-based virtualization capabilities of Intel® Virtualization Technology (Intel® VT). For information about setting up and configuring systems for virtualized environments, refer to the Intel vPro technology deployment guide for Intel VT.

information from leading IT service providers and corporations who have tested Intel AMT, visit the industry support section of the Intel Web site.

The rest of this section briefly describes critical IT challenges in enterprise environments, and the Intel AMT hardware-based capabilities that address those challenges. For additional information about Intel AMT or Intel vPro technology, visit the Intel Web site or contact your Intel representative.

Addressing critical IT challenges

The key to any company's success is the ability to manage and adapt to a changing and competitive environment, while keeping down costs and planning for the future. This includes managing and adapting to changing infrastructures and increased demands for IT services. As computer networks grow increasingly large and complex, the challenge of managing an IT infrastructure grows ever more difficult.

For example, shrinking transistors and new capabilities have significantly dropped the cost of PCs relative to the compute power they deliver. However, the cost of managing PCs has grown in opposite proportion. Today, the cost of managing PCs has become a significant percentage of the total cost of ownership of technology.

Two of the obvious solutions to meeting the increased demands for IT services are to:

- Automate more tasks.
- Allow more tasks to be performed from a remote, centralized location.

The problem is that a certain segment of PCs has traditionally been unavailable for remote management by software-based solutions. These PCs include systems that are powered off, whose OS is not responding or inoperative, whose hardware (such as a hard drive) has failed, or whose software agents are disabled or missing.

When PCs cannot be remotely managed or secured, IT technicians must make costly deskside visits to inventory, service, repair, or remediate machines. In addition, unmanaged machines put businesses are at risk from security threats, and expose corporate officers to liabilities from inaccurate asset tracking and software licensing. An unmanaged environment can be a costly expense.

A critical IT challenge

PCs that can't be found, can't be managed, and an unmanaged environment is an unsecured environment. One of the most critical challenges facing IT organizations is managing PCs that have traditionally been unavailable to the remote management console.

Extensive research into IT challenges

To help resolve enterprise IT challenges and identify the most critical areas where IT organizations need improved management capabilities, Intel conducted extensive research. This included interviewing and surveying numerous IT organizations in leading corporations around the world.

The results were surprisingly consistent, even across industries. Primarily, IT organizations reported a critical need for faster and more accurate asset management; reduced downtime and fewer desk-side visits for system maintenance and repair; and better security capabilities to help prevent and respond to malicious attacks.[1]

[1] Source: The white paper titled, "Reducing Enterprise Management Costs with Intel® Active Management Technology," 2006, Intel

Remote manageability built in

The powerful new manageability and security capabilities of Intel AMT are designed to meet some of the most critical IT challenges of today's organizations. The new capabilities are built directly into the PC's hardware and firmware, and are delivered in a high-performance, energy-efficient yet mainstream package – an affordable solution to deploy across an enterprise.

Because the capabilities of Intel AMT are designed into the PC, they are available to IT technicians – either manually or via third-party software – anytime. As long as the PC is connected to a power source and plugged into the network, the capabilities of Intel AMT are available to authorized IT technicians. This gives technicians new mechanisms to communicate with and service PCs in any business environment, from large enterprises, to distributed enterprises, to small- and medium-sized business environments.

IT organizations can now significantly reduce manual processes; increase automation for inventory, update, and upgrade tasks; shift more work off-hours; and minimize interruptions to business. The result is a more managed, more secured, more efficient infrastructure that helps reduce the cost of deploying and owning technology.

H/W technology enhances software

Intel AMT can enhance software management solutions so that software applications can communicate with and manage PCs even if PC power is off, the OS is unavailable, or management agents are missing. Even if hardware has failed, IT technicians can now use management software to receive alerts, upload hardware asset information, access BIOS information, and perform other tasks.

Intel AMT capabilities – always available

Intel AMT is part of the Intel® Management Engine. The Intel AMT capabilities are designed into system hardware and firmware. The most significant advantage of these capabilities is that, because they are based in hardware and firmware, they are available anytime, even if the PC is powered off, the OS is unavailable, or management software agents are missing. Even if hardware (such as a hard drive) has failed, a third-party management software (refer to Figure 2-1) can remotely power up the PC, let you watch

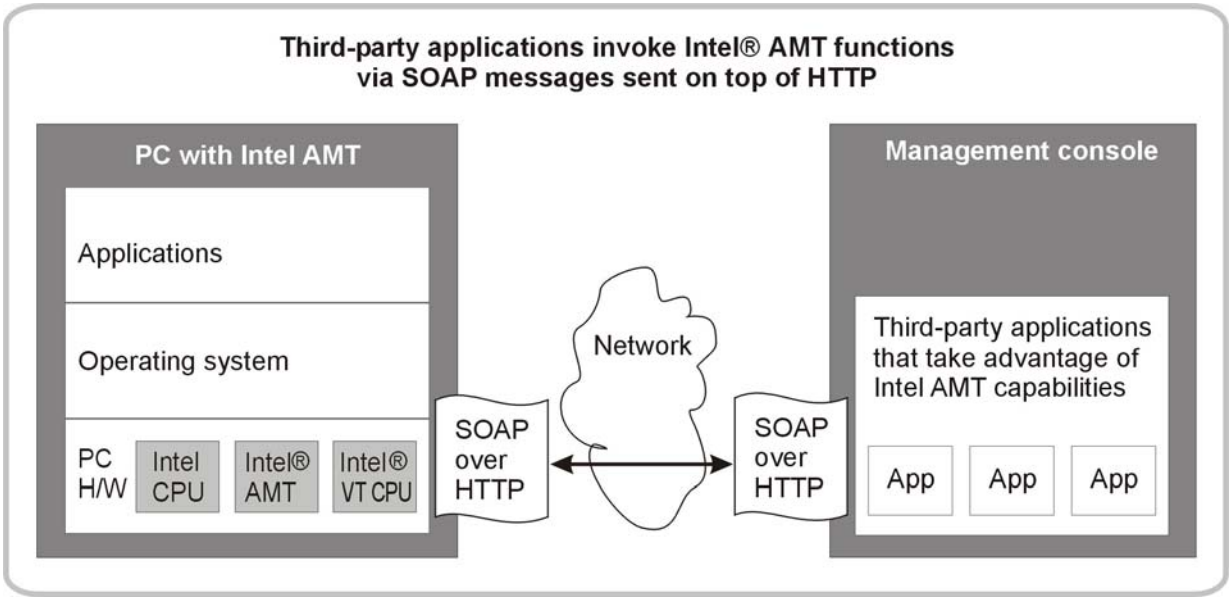

Figure 2-1. Remote management of PCs. Third-party applications can remotely manage PCs with Intel AMT using SOAP (simple object access protocol).

as BIOS, drivers, and the OS attempt to load, allow access to hardware asset information, and allow you to perform other monitoring, diagnostics, repair, and remediation, as needed, and without leaving the service center.

To understand how best to deploy Intel AMT-enabled PCs, you must first understand the hardware-based capabilities, how they could fit securely into your managed environment, and how they could be used most effectively to improve your IT processes. The capabilities include:

- **Remote-communication channel,** which runs "under" or "outside" the OS (refer to Figure 2-2 on the next page), so authorized IT administrators can communicate with the PC anytime. The remote communication channel is based on the TCP/IP firmware stack, not on the software stack in the OS. It works even if the OS is inoperative, and even if PC power is off. As long as the PC is connected to a power source and plugged into the network, an authorized technician can use management software to remotely manage PCs.
- **Access to hardware asset information,** so IT technicians can identify compatibility issues and determine the manufacturer and model of particular parts that needs replacing. This information is stored in the Intel AMT nonvolatile memory, and automatically updated each time the system goes through power-on self-test (POST). The nonvolatile memory draws a tiny amount of current even when the PC is powered off, in order to keep this information accessible at all times.

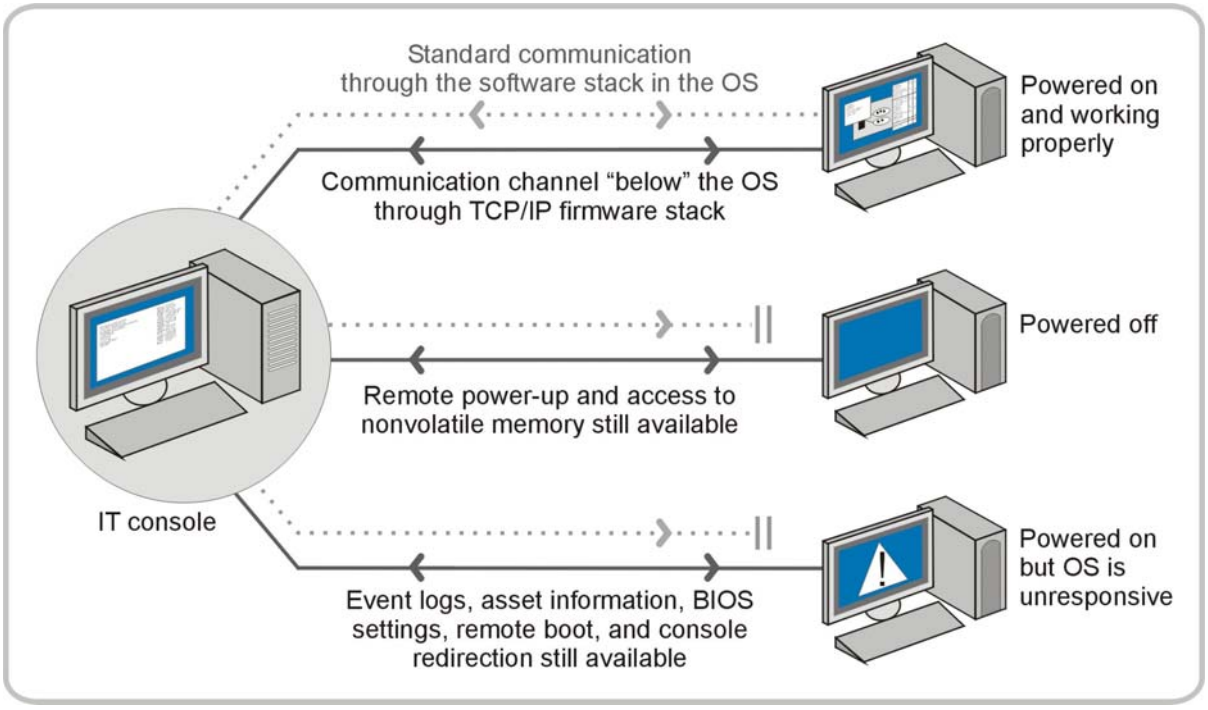

Figure 2-2. Remote communication channel. The hardware-based communication channel runs outside the OS, so it remains available to authorized technicians, even when the PC is powered off or its OS is not available.

Nonvolatile memory

The Intel AMT nonvolatile memory is divided into three segments:

- Storage for the signed, encrypted Intel Management Engine and the information used by Intel AMT.
- Storage for hardware asset information, BIOS configuration information, the unique ID, the event log, and other system information.
- The 3PDS – storage configurable by authorized IT administrators for use by third-party software.

- **Access to third-party data storage (3PDS),** a persistent, nonvolatile memory space where third-party vendors can store information, such as software version numbers, .DAT file information, machine IDs, pointers to database information, or other data. IT technicians can upload the information in this memory to assist in software-asset inventories, application or OS migrations, problem resolution, and so on. This helps minimize reliance on local software agents to store and retrieve data to help prevent accidental data loss.
- **Access to preboot BIOS settings,** for verifying configuration information and changing settings as needed to help resolve problems.
- **Remote power-up,** so IT technicians can power up, power down, power cycle, or reset PCs from the management console.

- **Remote/redirected boot,** through integrated drive electronics redirect (IDE-R), so authorized IT technicians can remotely boot a PC to a clean state, or redirect the boot device for a problem PC to a clean image on local storage, on a CD at the help desk, or to an image on another remote drive.
- **Console redirection,** through built-in serial-over-LAN (SOL) capabilities, so IT technicians can guide the PC through a troubleshooting session without user intervention, and without leaving the management console.
- **Always-available alerting,** so the PC can send alerts and SNMP (simple network management protocol) traps to the management console anytime. This gives an IT technician visibility of fan speeds, temperatures, case intrusions, hardware failures, OS lock-ups, and other critical events as they occur.
- **Persistent event logs,** so IT technicians can access the list of events that occurred before a hardware or software problem became apparent. The event log is accessible if the PC is powered down, even if the OS becomes inoperative.
- **Agent presence checking,** part of system defense (refer to Figure 2-3). This capability uses hardware-based timers, so third-party applications and management software can check in with the system at IT-defined intervals. IT administrators no longer need to wait for slow, multiple serial polls to find out about a potential problem.
- **Network outbreak containment,** part of system defense (refer to Figure 2-3). This capability uses hardware-based filters to check inbound and outbound traffic for known threats, and circuitry that allows IT to use policy-based rules to set rate-limits or isolate systems by disconnecting network communication at the software stack in the OS.

TLS required

In enterprise mode, TLS is required for some advanced capabilities, such as SOL, IDE-R, agent presence, and network outbreak containment.

The new hardware-based capabilities of Intel AMT offer a new level of remote management and security for PCs in any business environment.

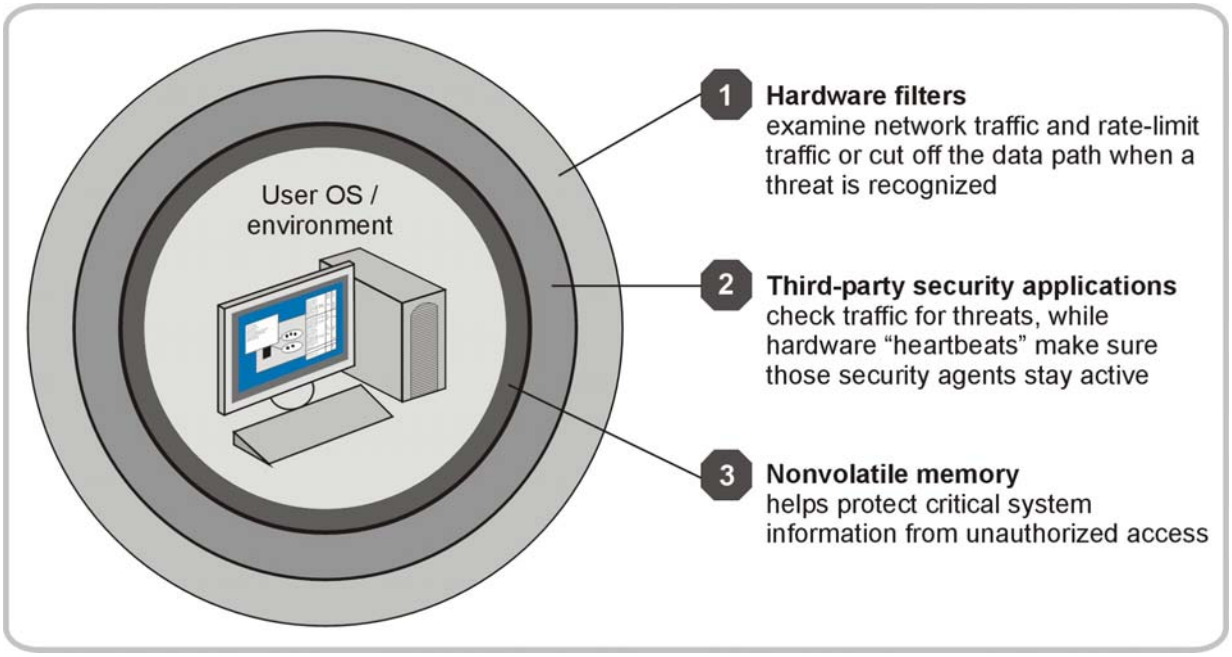

Figure 2-3. Three layers of defense. Intel AMT offers three layers of hardware-based defense, with agent presence checking, network outbreak containment (filters and the IT-defined policies for filtering network traffic), and tamper-resistant nonvolatile memory for critical system information.

Virtualization capabilities also built in

PCs with Intel vPro technology also include the embedded, hardware-based virtualization capabilities of Intel Virtualization Technology (Intel VT). These capabilities allow IT organizations to install a third-party management or security "virtual appliance" on the PC in a dedicated, hardware-based space. This can give an IT organization a tamper-resistant service OS from which to protect management software and processes, and manage, repair, and remediate a user OS.

For general information about Intel VT, refer to the Intel VT white paper on the Intel Web site. You can also visit the Intel Web site for information about virtual appliances provided by specific third-party vendors.

Deploying PCs with Intel VT

For information about setting up and configuring PCs with Intel vPro technology for virtualized environments, refer to the Intel vPro technology deployment guide for Intel VT.

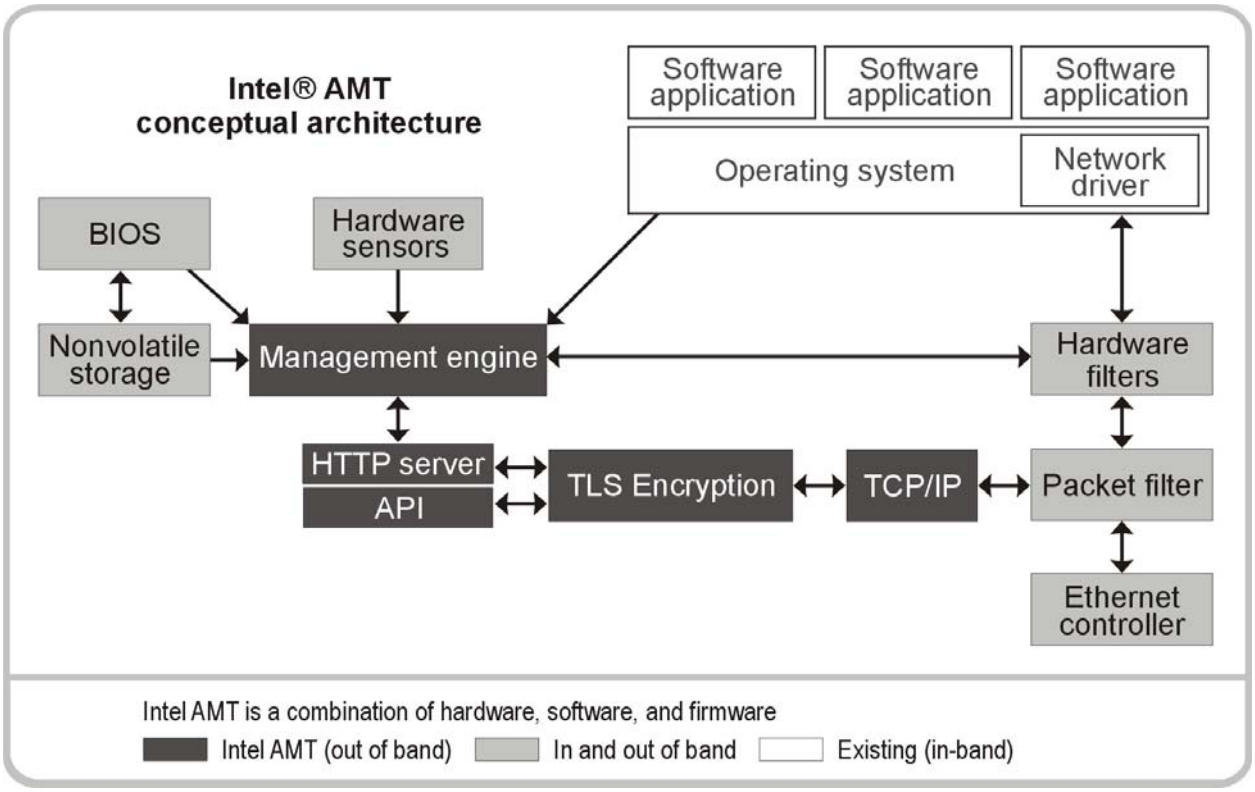

Figure 2-4. Intel AMT conceptual architecture. Intel AMT is a combination of hardware, software, and firmware that provides new remote-management capabilities for IT technicians.

Architecture and services

Intel AMT is a powerful set of capabilities for IT technicians. This discussion provides a brief overview of the architecture and functional services of Intel AMT.

Conceptual architecture

Intel AMT is part of the Intel Management Engine; technology built directly into the hardware and firmware of the PC. Figure 2-4 (above) shows the conceptual architecture for Intel AMT.

For network traffic, such as communication with the management console, the host OS (the PC's operating system) and the management engine use the same Ethernet controller. This allows Intel AMT hardware and firmware to still access the network through the Ethernet device, even if the OS is unavailable.

For in-band communicationbetween the OS and management engine, the OS uses the management-engine interface (MEI) to communicate to the management engine.

Out-of-band communication

Intel AMT uses an Ethernet controller directly, without going first through the OS. This provides IT technicians with "always-available" access to Intel AMT capabilities, even if the OS is unresponsive.

TLS and HTTP

If Intel AMT is configured to use TLS, a secure connection between the management console and Intel AMT will be established with each endpoint authenticating itself to the other endpoint. If TLS is disabled, Intel AMT will still use HTTP digest authentication to help secure communications.

Web services architecture

Intel AMT uses the web services standard for communications with other management applications (such as the management console, or software agents on the PC). This requires that Intel AMT functions are invoked by sending SOAP (simple object access protocol) messages on top of HTTP transport protocol. SOAP uses XML for serializing the remote procedure calls and objects.

Web services for Intel AMT have four major components (refer to Figure 2-5, on the next page):

- **Connection layer,** which provides a mechanism to connect to the Intel AMT web server, which is part of the Intel Management Engine. This layer also implements Intel AMT security. The connection layer is built on top of TCP/IP and TLS to provide a secure connection between the management engine and the remote-management console.
- **Transport layer,** which provides a way to carry serialized information from the application to the Intel AMT web server. Intel AMT uses HTTP for communication between the remote-management console (or software agent on the PC) and the Intel Management Engine.
- **Serialization.** Intel AMT uses SOAP for serialization and remote procedure calls. Applications that invoke an Intel AMT function do so by sending a SOAP message that represents the function to be invoked.
- **Remote interfaces.** Intel AMT uses WSDL (Web services description language) to describe its services.

Management services

Intel AMT has the following management services:

- **Security administration service –** provides an interface that allows you to configure the PC's access control list.
- **Network administration service –** provides a mechanism that allows you to specify the PC's network properties, including networking mode (static IP or dynamic IP), hostname, domain name, and other parameters.
- **Storage administration service –** provides mechanisms for reconfiguring global parameters that govern the allocation and use of third-party nonvolatile storage.
- **Hardware asset service –** provides mechanisms for retrieving a hardware information tag from nonvolatile memory.
- **Remote control service –** implements a mechanism to acquire information about remote management capabilities and invoke those capabilities. The capabilities include remote control and boot options, including SOL, IDE-R, power up, power down, power cycle, and reset.

TLS required

In enterprise mode, TLS is required for some advanced capabilities, such as console redirection (SOL), remote boot (IDE-R), agent presence, and network outbreak containment (NOC).

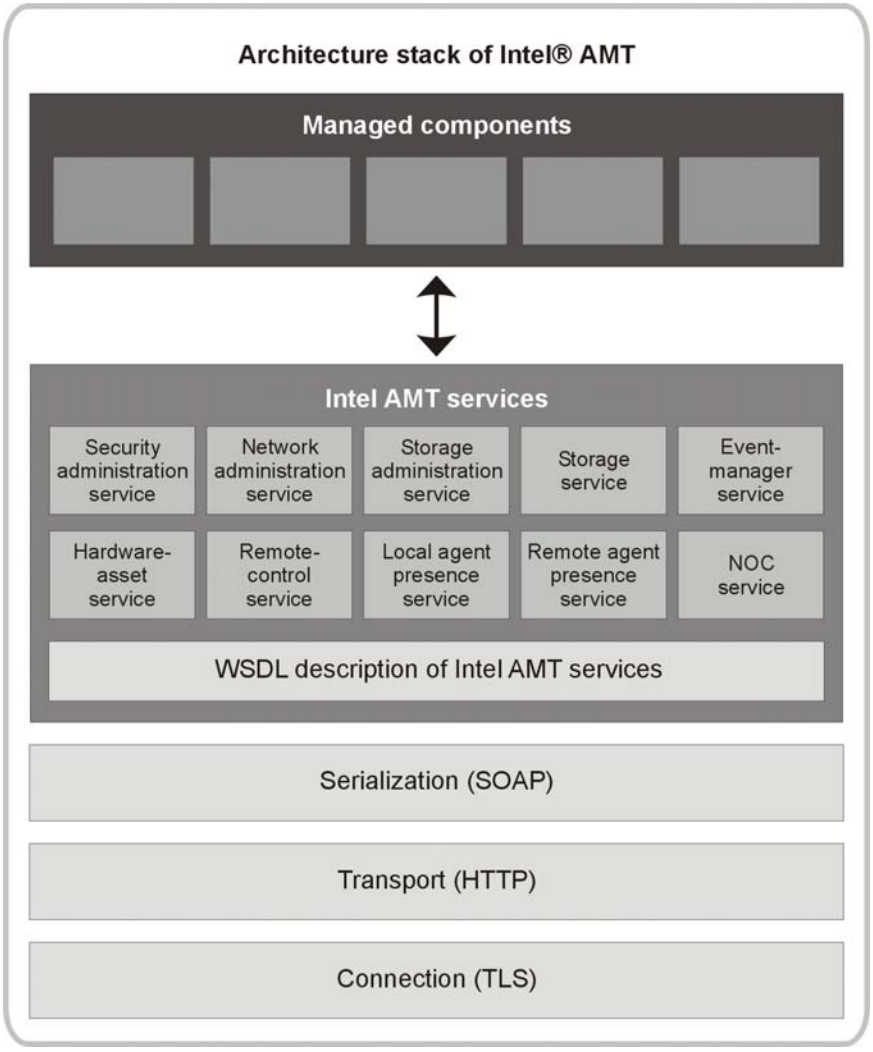

Figure 2-5. Architecture stack for Intel AMT services. Web services for Intel AMT have four major components.

- **Storage service –** provides mechanisms for allocating, using, and managing blocks of the nonvolatile storage in the PC. This storage can be accessed even when the PC is powered off, the OS is unresponsive, or management agents are missing.
- **Event manager service –** allows you to subscribe or unsubscribe to events from the PC.
- **Local agent presence service –** gives third-party applications installed in the PC the ability to register with the "watchdog" services of Intel AMT. These services include "heartbeat" presence checking for registered applications and network outbreak containment and event-manager policies in case of a change in the application state.

- **Remote agent presence service –** gives third-party applications running on the remote system the ability to register with the "watchdog" services of Intel AMT.
- **Network outbreak containment service –** used by remote or local applications (management agent presence) to apply filters, rate-limits, and isolation policies to network traffic.

Intel AMT is language-agnostic

Intel AMT is OS-agnostic for manageability, but is also language-neutral for applications. You can write applications to take advantage of Intel AMT capabilities in any programming language.

Language support

Intel AMT is built on Web Services technology, a language-neutral technology. You can write applications that access Intel AMT functions (with a SOAP stack) in any language, such as C/C++, Java, C#, Visual Basic, TCL, Python, and so on. Figure 2-6 shows the remote-management application stubs for Intel AMT capabilities

To write an application that takes advantage of an Intel AMT function, follow these general steps:

1. Generate client side stubs in the desired language from the WSDL description of the Intel AMT service that you want to use.
2. The stub will provide following functions:
    - A function to connect to the PC, given its network address.
    - A wrapper function for each Intel AMT function described in the WSDL description of the Intel AMT service.
3. Create the application that calls the Intel AMT function.
    - Call the function that connects to the PC.
    - Call the wrapper functions in the stub to invoke the Intel AMT function you want to use.

The stub will create the SOAP message and send it to the PC. Upon receiving the SOAP message back from the PC, the stub will convert the message into the data structure in the specified programming language. Your applications should then be able to parse the results from the PC.

Client-side stubs

The stub provides a function to connect to the PC, and a wrapper function for each Intel AMT function described by the corresponding Intel AMT service.

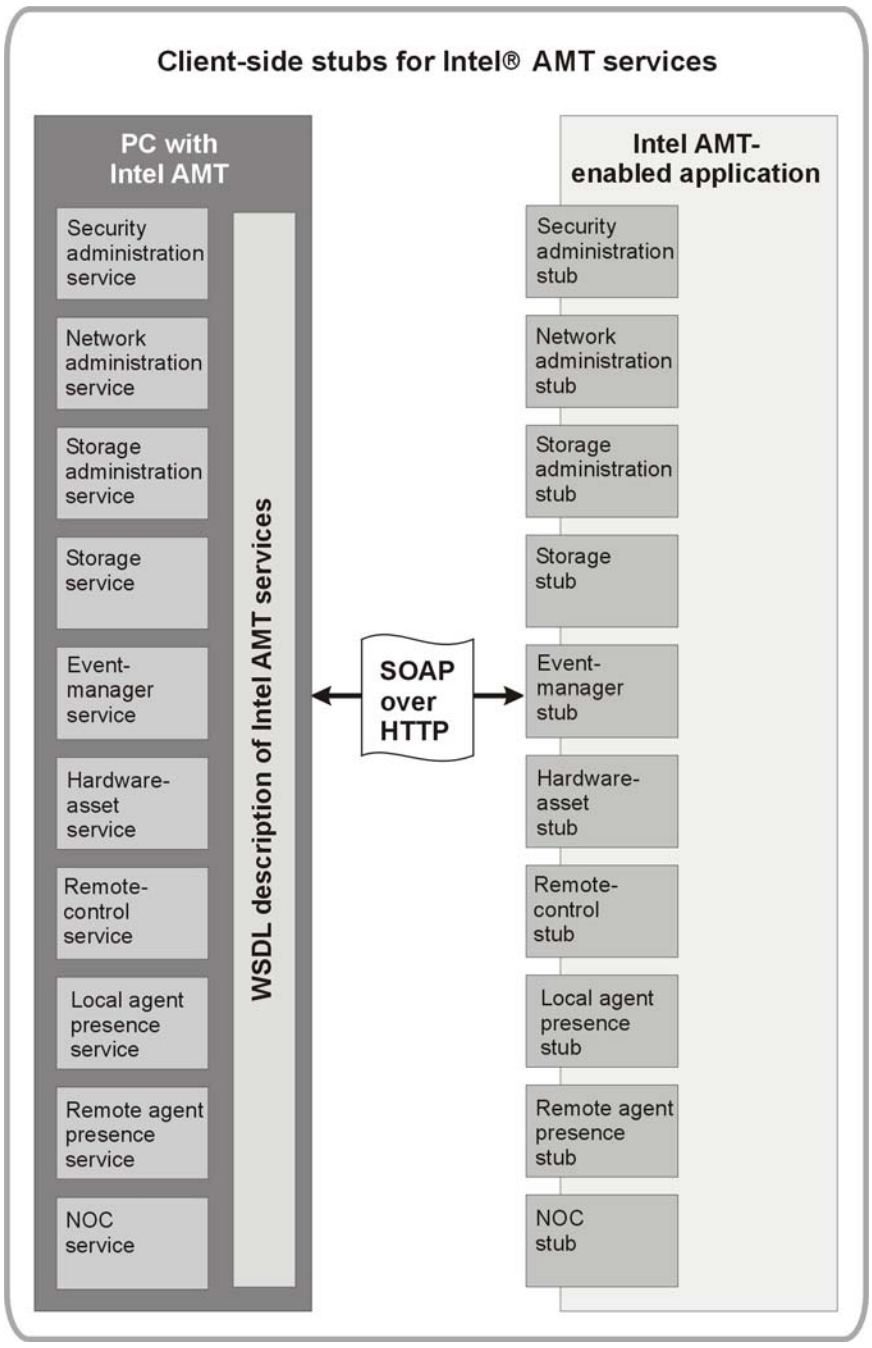

Figure 2-6. Remote-management application stubs. You can generate client-side stubs to take advantage of Intel AMT capabilities.

For more information

The next several sections of this guide provide reference information about security methodologies and techniques, networking requirements, setup and configuration parameters, and configuration management.

Usage models and some typical use cases for Intel AMT are described in the appendices of this guide. These use cases can help you identify processes where Intel AMT can offer improvements, and give you a starting point for building a proof-of-concept (POC) evaluation or pilot study. Case studies, evaluation reports, and white papers about POC tests and pilot studies in customer environments can be found on the Intel Web site.

Section 3
Security Methodologies and Technologies

Intel® AMT

Intel® Active Management Technology (Intel® AMT) is one aspect of the new hardware-based capabilities of Intel® vPro™ technology

Terminology

- CS – configuration service
- ME – management engine
- PC – a PC with Intel AMT
- PID – provisioning ID
- PPS – provisioning passphrase
- TLS – transport layer security

Introduction

Security is a key consideration for remote management of PCs in any business. Because PCs with Intel AMT deliver "always-available" capabilities to authorized IT technicians, it is critical that security for these systems be robust and set up properly.

Caution

Intel AMT devices should be configured on an isolated network during initial setup, in order to minimize exposure of sensitive information, such as passwords, to unauthorized users or other security threats. An isolated network is critical because, during initial setup and before transport layer security (TLS) certificates and keys are configured, the configuration traffic is sent without encryption. Once TLS authentication is in place, typical security procedures can be applied.

Note

If the configuration service (CS) requires access to both a user network and the isolated configuration network, make sure to equip the server with more than one network interface. You can then use one network device to establish isolated network connections to the PCs to be configured. You can use the second network device to connect to the user network.

This section explains the security methodology, authentication protocols, and processes used to establish security for remote management of PCs with Intel AMT.

Security for remote-management features

Intel AMT allows IT administrators to perform many remote tasks for their networked computing assets, regardless of PC power state or the state of the OS. The channel through which these capabilities are delivered must be appropriately secured in order to help maintain security for the network as a whole.

The communication and manageability capabilities built into PCs with Intel AMT are secured through a variety of robust schemes.

Remote communication

The remote-communication channel in these PCs runs outside the OS, and uses the TCP/IP stack in system firmware, rather than the software stack in the OS. This allows IT technicians to communicate with the PC even if PC power is off or the OS or management agents are compromised or inoperative. The remote-communication channel is secured through TLS to help prevent IP spoofing. Commands sent to Intel AMT via SOAP (simple object access protocol, a Web communication protocol) are authenticated through HTTP digest and Kerberos.

Remote power-up

PCs with Intel AMT give authorized IT technicians the ability to remotely power-up PCs for streamlined, automated, and off-hours security updates, patch management, and maintenance. Security for this capability is provided through TLS, HTTP authentication, and enterprise-level authentication using Microsoft Active Directory* (Kerberos).

Persistent, nonvolatile memory

Persistent, nonvolatile memory is a tamper-resistant space divided into three key areas. The first section in this nonvolatile memory is used for the Intel® Management Engine and for information used by Intel AMT. The other two areas are used for the system's hardware asset information and event logs; and for third-party information. The management engine and Intel AMT information are signed and encrypted. Third-party vendors are responsible for the security (such as signing and encrypting) of the data they store in nonvolatile memory. Access to all nonvolatile memory is controlled by an access control list (ACL).

* Other names and brands may be claimed as the property of others.

Intel AMT

Intel AMT is part of the Intel Management Engine. When you perform the setup and configuration procedures in this guide, you are setting up and configuring Intel AMT, not the management engine (or PC) in general.

Terminology

- ACL – access control list

Terminology

- IDE-R – integrated drive electronics redirect
- NOC – network outbreak containment
- PET – platform event trap
- PXE – preexecution boot environment
- SNMP – simple network management protocol
- SOL – serial over LAN
- WOL – wake on LAN

TLS must be enabled for system defense

System defense capabilities, such as network outbreak containment and agent presence, are powerful new options for helping secure PCs. TLS must be enabled in order for you to use these new, hardware-based defenses.

Intel® Virtualization Technology

For information about the virtualization capabilities built into PCs with Intel vPro technology, refer to the Intel Web site or to the deployment guide for Intel® Virtualization Technology (Intel® VT).

Always-available alerting and event logs

Because PCs with Intel AMT can respond to the remote management console anytime, they can send platform event traps (PETs) via simple network management protocol (SNMP) anytime.

Events are stored in nonvolatile memory, which is controlled by an access control list. The persistent event log can be used for verification of PET alerts and events.

Access to the event log is secured through an access control list, as well as through HTTP authentication, TLS, and Kerberos.

Remote troubleshooting and system recovery

Capabilities that improve remote troubleshooting, diagnostics, repair, remediate, and rebuild processes are delivered through remote boot (remote/redirected boot) and console redirection, as well as through the persistent event log. Remote boot is provided through integrated drive electronics redirect (IDE-R). IDE-R is more secure than preexecution boot environment (PXE) or wake on LAN (WOL). Console redirection is provided through serial over LAN (SOL). The remote-boot and console-redirection capabilities are secured through HTTP authentication and TLS.

System defense

PCs with Intel AMT subscribe to the philosophy that a well-secured PC helps improve the security of the network as a whole. Advanced capabilities in these PCs help improve system defense through hardware-based filters for inbound and outbound network traffic, built-in isolation circuitry (“network outbreak containment” or NOC), and hardware-based timers for agent presence checking. These capabilities are embedded in hardware and so are invisible and tamper-resistant to users, hackers, viruses, worms, and other security threats.

Protected virtual partitions

Hardware-based virtualization capabilities are also built into PCs with Intel AMT. These capabilities give third-party software vendors a dedicated space in which to improve protection of management applications and processes.

Terminology

- AES – advanced encryption standard
- RSA – an abbreviation comprised of the initials of the last names of the founders of this security method.

* Other names and brands may be claimed as the property of others.

Highlights of security technologies

To help ensure that only authorized users have access to critical capabilities, and to protect against network attacks and/or technology misuse, PCs with Intel AMT employ robust access control and privacy mechanisms.

Some of the highlights of Intel AMT security are:

- Transport layer security protocol to secure communications over the out-of-band network interface. The TLS implementation uses AES 128-bit encryption and RSA keys with modulus lengths of 2048 bits.
- HTTP digest authentication protocol as defined in RFC 2617. The remote-management application authenticates IT administrators (or other users) who manage PCs with Intel AMT.
- Single sign-on to Intel AMT with Microsoft Windows* domain authentication, based on the Active Directory and Kerberos protocols.
- A pseudo-random number generator (PRNG) in the firmware of the Intel AMT system, which generates high-quality session keys for secure communication.
- Only digitally signed firmware images (signed by Intel) are permitted to load and execute.
- Tamper-resistant and access-controlled storage of critical management data, via a nonvolatile data store in the Intel AMT hardware.
- Access-control lists for Intel AMT realms and other management functions.

The next discussion provides an overview of the approaches and technologies used to establish security for the capabilities of Intel AMT.

Overview of security technologies

This discussion describes the methods and implementation of security technologies for PCs with Intel AMT. This discussion covers two general areas:

- Secure communications and authentication
- Implementation of security technology

Information about the actual processes followed to establish secure networking and communications for IT-automated, manual, and factory-automated setup, and for automated configuration is provided later in this section, after this general discussion.

Secure communication and authentication

Intel AMT supports TLS mutual authentication, as well as HTTP digest authentication. TLS and mutual authentication are both optional.

A critical portion of the setup and configuration activity is the exchange of secret keys and installation of certificates that are required to implement both TLS server authentication and TLS mutual authentication. Please note the following:

- Intel AMT starts the configuration process by exchanging messages with a configuration server that are not encrypted. Therefore, Intel AMT should be configured on an isolated network.
- Intel AMT is initialized with a public password and a private key (a PID/PPS pair). The configuration server must have these two values, as well as the internal unique identifier of the PC with Intel AMT, in order for the configuration process to start. The secure handshake performed using this information allows an Intel AMT configuration process to take place on an open enterprise network.
- TLS requires that Intel AMT have a server signed certificate that that is traceable to a certificate authority. The configuration service (CS) implements the process required to request, sign, and install a server certificate in Intel AMT.
- Mutual authentication requires that Intel AMT have a server signed certificate, and the remote management console have a client certificate. Each local agent may also require a certificate if its communication model is set up for TLS mutual authentication.

Certificates for third-party applications

Refer to the documentation for your management console for information about application requirements of security certificates.

TLS protocol

The TLS protocol is defined in RFC2246 and RFC3546. Refer to those online documents for more information and for details about TLS.

Transport layer security

The TLS protocol provides communication security and privacy over the Internet and enterprise networks. The protocol supports server and client channel authentication.

The TLS protocol is application independent. It allows other protocols, such as HTTP, to be transparently layered on top.

The TLS protocol is able to negotiate encryption keys as well as authenticate the server before data is exchanged by higher-level applications. The TLS protocol maintains the security and integrity of the transmission channel by using encryption, authentication and message authentication codes.

Each time a server and client communicate, the TLS protocol establishes a secure channel of communication between the client and server, and consists of two phases:

- Required: server authentication
- Optional: client authentication (mutual authentication)

In the first phase, the server sends its certificate and its cipher preferences in response to a client's request. The client then generates a master key, which it encrypts with the server's public key, and transmits the encrypted master key to the server. The server recovers the master key and authenticates itself to the client by returning a message authenticated with the master key.

In the optional second phase of authentication, the server sends a challenge to the client. The client authenticates itself to the server by returning the client's digital signature on the challenge, as well as its public-key certificate. A variety of cryptographic algorithms are supported by TLS. Subsequently, the client and server use keys derived from the master key to encrypt and authenticate the exchange of data between themselves.

Preshared-key TLS (TLS-PSK)

The preshared-key TLS is a set of cipher suites added to the TLS protocol. This set of suites allows the TLS protocol to function between two nodes, without the use of public key technology.

The preshared-key TLS relies on the assumption that the two nodes that are establishing the TLS-PSK session already share a common secret key. The secret key is typically installed on the two systems, independent of the network, by a system administrator using secure methods.

Digitally signed code

One of the major issues in using generally available software (such as software available over the Internet) is whether users can trust such software. There are two issues that must be addressed to establish trust:

- Ensuring authenticity. There must be a way to assure of where the code came from. Assurance is typically provided through the use of digital signatures.
- Ensuring integrity. There must be a way to verify that the code hasn't been tampered with since its publication.

The use of digital signatures on the code assures recipients that the code does come from the specified source intact.

Digital signatures are created using a public-key signature algorithm, such as the RSA public-key cipher. In practice, however, public-key algorithms are often too inefficient for signing long pieces of data (which in this case is code).

To save time, digital signature protocols use a cryptographic digest, which is a one-way hash of the code. The hash is signed instead of the code itself. Both the hashing and digital signature algorithms are agreed upon beforehand through this process:

1. The sender calculates a one-way hash of the code image.
2. The sender encrypts the hash with the private key, thereby signing the document.
3. The sender transmits the code and the signed hash.
4. The recipient produces a one-way hash of the code.
5. Using the digital signature algorithm, the recipient decrypts the signed hash with the sender's public key.
6. If the signed hash matches the recipient's hash, the signature is valid and the code is intact.

When application code (software) is associated with a publisher's unique signature, distributing software over an insecure medium such as the Internet is no longer an anonymous activity. The digital signatures ensure trust by allowing authentication of origin and integrity checking on the code.

Server and client

In single (server-side) authentication, Intel AMT acts as the server, and the management console acts as the client. Intel AMT has the certificate and authenticates the management console. In mutual authentication, both endpoints have certificates, and each must authenticate itself to the other endpoint.

TLS and HTTP

TLS is a transport protocol, while HTTP is an authentication protocol (like a log-in protocol). You can think of TLS as the encrypted communication tunnel, and HTTP as the authentication method for the endpoints using that tunnel. If TLS is disabled, Intel AMT will still use HTTP digest authentication to help secure communications.

SOL and IDE-R

Some Intel AMT capabilities, such as SOL and IDE-R, use TLS over TCP/IP, rather than HTTP authentication. HTTP is a communication method used for talking to or interfacing with the Web service. SOL and IDE-R sessions are set up using SOAP over HTTP, but the capabilities themselves do not use the Web service (via HTTP) for sending and receiving data to/from the Intel Management Engine.

HTTP digest authentication

The HTTP protocol provides for two authentication mechanisms: the HTTP basic authentication, and the more secure HTTP digest authentication. These mechanisms are detailed in RFC 2617.

HTTP basic authentication protocol provides for a challenge-response authentication mechanism. This mechanism can be used by a server to challenge a client, and used by a client to provide authentication information back to the server.

During HTTP basic authentication, the client sends its user-ID and password to the server. The server (Intel AMT) authorizes the client (the management console) only if the server can validate the user-ID and password. Otherwise, the server responds with an error code. The user-ID and password are sent across the wire, without any encryption, which makes the basic authentication scheme less secure than then HTTP digest authentication.

The HTTP digest authentication scheme is more secure than the HTTP basic authentication scheme. In HTTP digest authentication, the password is never sent from the client to the server in the clear. Instead, the server challenges the client with a random value (called a *nonce*). A valid response contains a checksum of the username, the password, the given nonce value, and some other data. In this way, the password is sent over the wire as a hash to prevent interception and reuse. Upon receiving the response, the server computes the checksum using the same inputs, and compares the computed checksum with the one received from the client. If they match, then the client is authenticated.

Kerberos authentication

Kerberos uses secret-key technology for encryption and authentication. Unlike a public key authentication system, Kerberos does not produce digital signatures. Instead, Kerberos was designed to authenticate requests for network resources.

About Kerberos

Kerberos is an authentication service developed by the Project Athena team at Massachusetts Institute of Technology (MIT). The first general use version of Kerberos was version 4. Version 5, which addressed certain shortfalls in version 4, was released in 1994.

Kerberos – RFC 1510

Some work has been done to incorporate public-key cryptography into Kerberos. For detailed information on Kerberos, refer to RFC 1510, the Kerberos Network Authentication Service (V5).

In a Kerberos system, there is a designated site on each network, called the Kerberos key distribution center (KDC). This site performs centralized key management and administrative functions. The KDC maintains a database containing the secret keys of all users and machines/servers, authenticates the identities of users, and distributes session keys to users and servers who wish to authenticate one another.

Caution:

Kerberos requires trust in a third part (the KDC). If the KDC is compromised, the integrity of the entire system is lost.

Public-key cryptography was designed precisely to avoid the necessity to trust third parties with secrets. Kerberos is generally considered adequate within an administrative domain or enterprise. However, it is more suitable to use public-key systems for enterprises that interact over the open Internet, and which have no inherent trust relationships between them.

Access control

Access control is the mechanism by which systems grant or revoke the right to access particular data, or perform particular actions. Typically, a user must first authenticate or log in to a system, using some authentication credentials such as a username and a password. The access-control mechanism then determines which operations the user may access by comparing the user's ID to an access control list (ACL) or database. An ACL specifies the privilege attribute(s) needed to access the object, as well as the permissions that can be granted with respect to the protected object to principals that possess privilege attribute(s).

Intel AMT allows individual usernames and passwords, or Windows domain groups to be assigned to various realms. A realm is a set of functions that are isolated from the rest of the functions. This allows an IT administrator to grant access to different features for different employees, or groups of employees, if needed. In general, best practices specify granting the fewest privileges necessary to any given user.

Security through configuration

When a PC with Intel AMT is powered on at the user desk, it should already be set up and have the data and technology resources required to appropriately configure Intel AMT. This ensures that the full spectrum of built-in features can be used to manage the system in a secure manner. These technology resources include unique and secure user-ID and password, secret keys, access control lists, and public-key certificates.

Implementation of security technology

This discussion explains how security technologies and methodologies are used during configuration or are implemented for PCs with Intel AMT.

TLS, HTTP, and Kerberos

Intel AMT uses many security features, including TLS authentication, HTTP digest, and Kerberos. This guide assumes that you are already familiar with these mechanisms.

TLS

Intel AMT uses TLS to secure its communication over the network. In TLS-secured communications, Intel AMT supports:

- the mandatory first phase of TLS authentication (i.e., server authentication), where the Intel AMT system sends its certificate to the client (the management console) for validation.
- the optional second phase of client-side TLS authentication, in which Intel AMT also requires a client-side certificate.

Authentication modes

Intel AMT supports both the mandatory first phase of authentication and the optional second phase of client-side authentication. Intel AMT supports additional authentication through HTTP digest authentication or Kerberos authentication protocols.

Further authentication of the IT administrator operating the management console (on the TLS client) is achieved using the HTTP digest authentication mechanism or Kerberos authentication protocols.

To support applications running on other devices, Intel AMT makes available a minimum of 48 simultaneous TLS sessions. At least one TLS session is always reserved so that the remote management application can always be accessed. The remaining TLS sessions can be used by any combination of the remaining applications (for example, multiple third-party data-store and agent-services TLS sessions). To facilitate access by all applications, appropriate timeout mechanisms are employed for each TLS session.

TLS for Intel AMT contains an RSA certificate or contains a certificate chain and the RSA private key that corresponds to the leaf certificate in the chain. The public key certificate and the private keys are used for TLS server authentication during the TLS handshake.

Table 3-1 lists the supported cipher suites and associated certificate types and key exchange algorithms.

Table 3-1. Cipher suites and recommended uses

Cipher suite	Certificate type and key- exchange algorithm	Recommended use
TLS_RSA_WITH_AES_128_CBC_SHA	RSA, X.509v3	Preferred, and used whenever possible.
TLS_RSA_WITH_RC4_128_SHA	RSA, X.509v3	Used only where the AES is not available.
TLS_RSA_WITH_NULL_SHA	RSA, X.509v3	Used only when regulatory requirements do not allow the use of the confidentiality.

The TLS implementation uses RSA keys with modulus lengths of 2048 bits, and public exponent values of 10001h (65537 decimal). The implementation supports a single certificate hierarchy with a minimum depth of two (for example, root and leaf). A certificate revocation list (CRL) is also supported to further validate host and Intel AMT system certificates.

Changing security certificates

Moving or renaming PCs

PCs that are moved to a new location require new certificates.

If a PC's operating-system name is changed or the PC is moved to a new location, you must reconfigure Intel AMT so that a new certificate can be generated with the new location information.

In dynamic IP environments, this can be performed by unconfiguring (partial unprovisioning) Intel AMT before the PC is moved. Once the PC is in its new location, Intel AMT can automatically reinitiate its configuration process, send its hello packets, and begin the automatic reconfiguration.

In static IP environments, once the PC has been moved, you must enter the new IP address. This is typically performed as part of the setup procedure. Once Intel AMT has been set up again, it can initiate and complete its own automatic configuration.

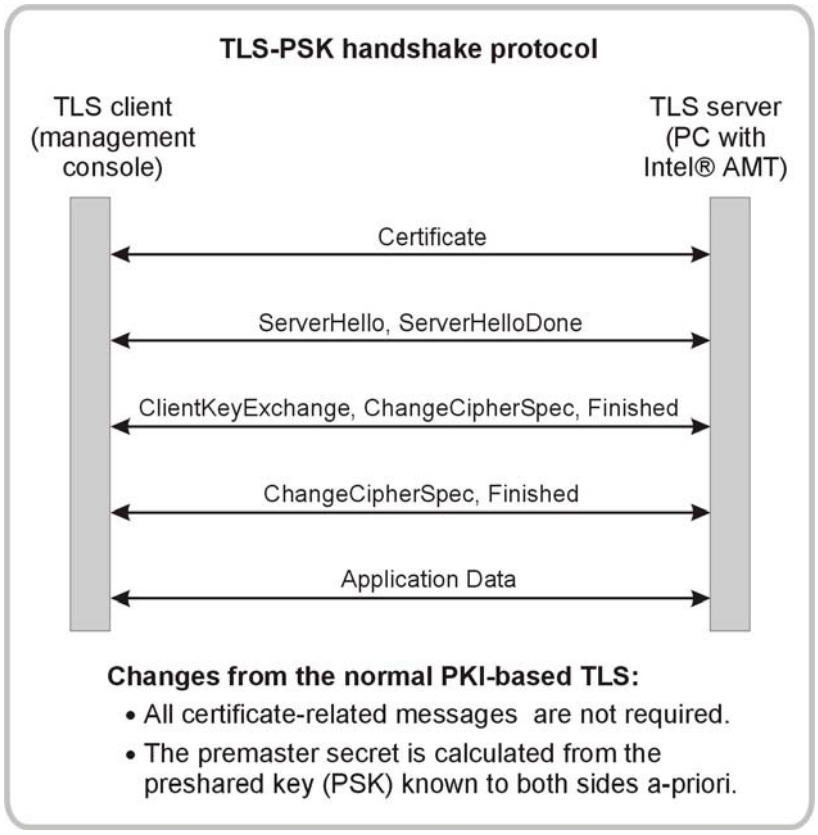

Figure 3-1. TLS-PSK handshake protocol. The TLS protocol handshakes are modified by the TLS-PSK protocol as per the IETF RFC definition.

TLS-PSK

Intel AMT uses the TLS-PSK protocol as the default protocol for configuring the system over the production network. TLS-PSK sessions are established between the configuration server and the Intel AMT in order to secure the communications between the two.

The TLS protocol handshakes are modified by the TLS-PSK protocol (as per the IETF RFC definition) as shown in Figure 3-1 (above). Table 3-2 lists the cipher suite and its encryption algorithm.

Table 3-2. TLS-PSK cipher suite

Cipher suite	Encryption algorithm	Recommended use
TLS_RSA_WITH_AES_128_CBC_SHA	AES_128_CBC	Preferred. This is the default protocol for configuring PCs.

HTTP digest authentication

Intel AMT uses the HTTP digest authentication scheme for authentication of the client (such as the remote console), before allowing access to the system. A challenge is sent to the client, and a response containing the digest of the password and other information, must be returned (refer to Figure 3-2, above).

UUID
The PC's machine ID is also known as its universal unique identifier, or UUID.

As shown in Figure 3-2, the PC stores the MD5 hash of the username, password, and the HTTP realm. The HTTP realm incorporates the PC's machine ID, which is unique for every system. This makes the hash value stored on every PC unique.

Should an attacker break into the PC's flash memory and seize this hash value, it is of no use in attacking other PCs with Intel AMT, even if the passwords of those systems happen to be the same.

The cryptographic hashing also ensures that the passwords cannot be reverse-engineered by gaining access to the hash value.

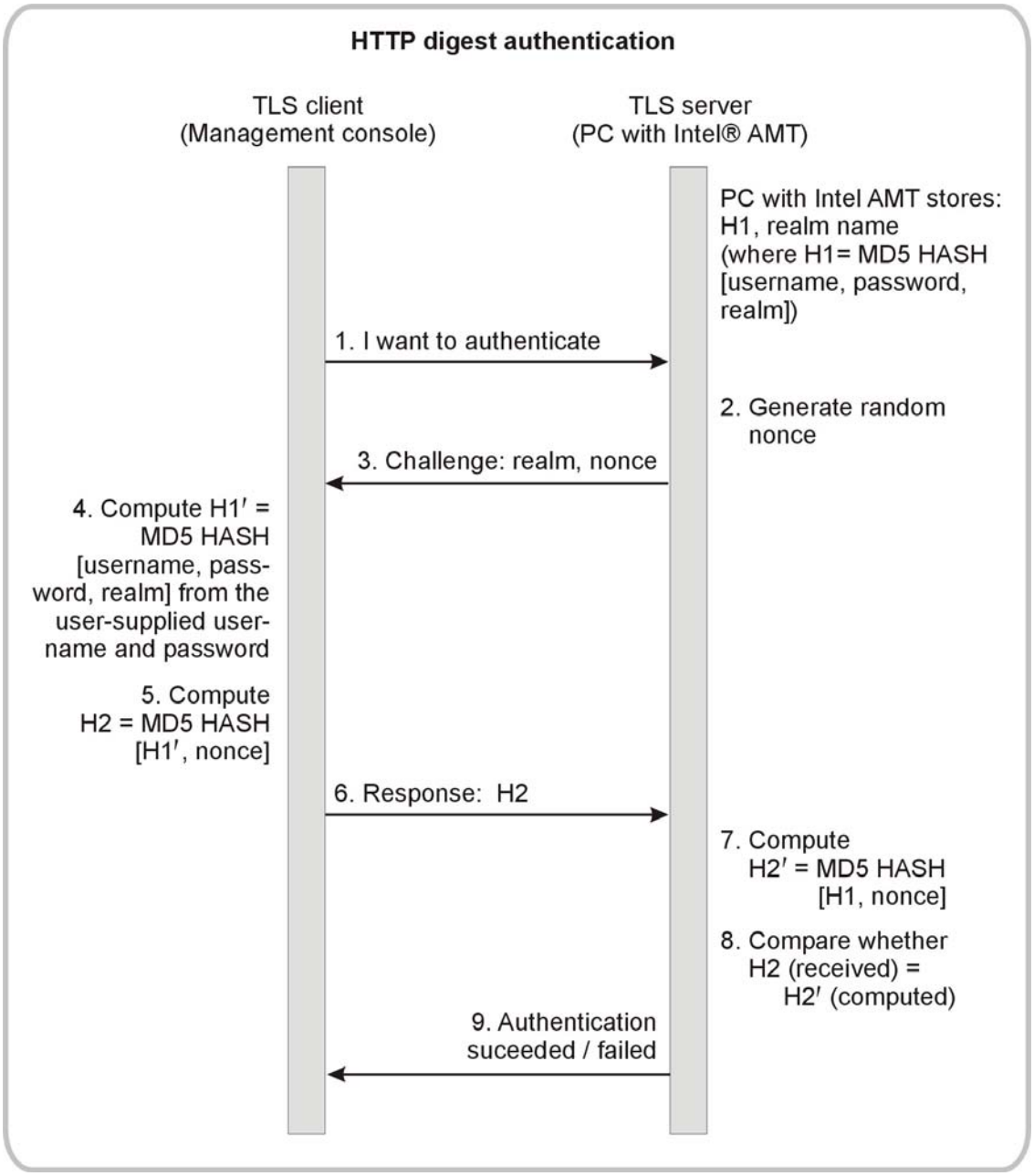

Figure 3-2. HTTP digest authentication. The authentication scheme requires that a challenge be sent to the client, and a response containing the digest of the password and other information, must be returned.

Kerberos authentication (integrated with Microsoft Active Directory)

The current authentication in Intel AMT is based on HTTP digest (RFC 2617), which in turn requires that each PC with Intel AMT be provisioned with at least one username-password pair.

In a large enterprise with thousands of systems, it will require a significant amount of management resources to configure and manage unique username-password pairs. This can lead to the use of weak passwords or common passwords used on multiple systems.

There are two general solutions to the password issue. Third-party software vendors can develop components that effectively manage passwords without compromising the security of the enterprise. Or, IT departments can integrate the authentication framework of these PCs with Windows domain authentication (managed by Active Directory) based on Kerberos protocol.

Best practices

Best practices recommend that you leverage Windows authentication to simplify adding and removing Intel AMT management privileges for users and improve password-management.

Integrating the authentication framework of these PCs with Windows domain authentication provides for a standard and single sign-on style authentication to the PC. This eliminates the need for third-party applications (including configuration services) to manage unique and strong username-password pairs for all systems with Intel AMT. Authentication to PCs with Intel AMT will be as strong and secure as authentication to the Windows domain. Also, administrators who manage these systems need only log into the Windows domain to gain access to the Intel AMT-enabled device.

The Windows infrastructure is currently the mostly widely deployed infrastructure in industry. Integrating Windows authentication into Intel AMT will cater to the majority of the consumer base.

There are several benefits of using the Kerberos authentication that is already integrated with Active Directory:

- If an IT administrator is logged into the Windows domain using his username (the domain-username, such as *amr/john*) and password, he is able to automatically authenticate the PC. This authentication is done behind the scenes, without the need to supply another password.
- An IT administrator is allowed or denied privileges to manage a PC based on his membership to a group in Active Directory. This ensures that, when an administrator should no longer manage one or more PCs with Intel AMT, his privileges to do so are revoked simply by removing his membership from the group

- PCs with Intel AMT are able to ascertain the identity of the administrator attempting to gain access to the device, and can apply access control for that user. The philosophy is that not everyone who is successfully authenticated is allowed access to all resources within Intel AMT. The authorization that a given user has is governed by an access control list (ACL) stored in nonvolatile memory in the PC
- Kerberos is standards-based:
  - Kerberos v5 – RFC1510
  - Kerberos v5 over GSS-API Mechanism – RFC1964
  - GSS-API SPNEGO Mechanism – RFC2478
  - SPNEGO over HTTP

The next discussion explains login mechanisms used by Intel AMT.

Login mechanisms

Intel AMT enforces certain password requirements and includes a login-backoff mechanism to help reduce login vulnerabilities to malicious attacks.

Password strength

Intel AMT requires that passwords used for authentication to the PC meet the following minimum criteria. Passwords must:

1. Be at least 8 characters long.
2. Include only valid characters. Allowed characters are 7-bit ASCII characters in the values of 32-126 inclusive.
3. Not include invalid characters. The following characters are **not** allowed:
   - " (left double quote)
   - . (period)
   - , (comma)
   - : (colon)
4. Have at least one digit character (0, 1, 2, …, 9).
5. Have at least one 7-bit ASCII non-alphanumeric character (such as ! or $).
6. Contain both lowercase (a, b, c, ...z) and uppercase (A, B, C, ... Z) Latin characters, or non ASCII characters (UTF+00800 and above).

These restrictions, which are enforced by Intel AMT, help to reduce susceptibility of passwords to offline dictionary attacks.

Login-backoff mechanism after failed login attempts

Intel AMT helps prevents online attacks to systems by including a "back-off" mechanism. The back-off mechanism is triggered by a certain number of successive failed login attempts. This feature substantially impedes a system attack using password guessing.

If an attacker tries to login to the PC by guessing a password, and Intel AMT detects ten successive login failures, further login attempts are disallowed for a period of time. The timeout period starts at 5 seconds and reaches 80 seconds during a continuous attack. After one hour of no attack, the backoff mechanism is reset.

Realms, nonvolatile memory, and access control

Intel AMT includes several mechanisms, such as realms with access-control lists, designed to help secure access to the powerful remote-management capabilities.

Realms

Intel AMT allows individual usernames and passwords, or Windows domain groups to be assigned to various realms. A realm is a set of functions that are isolated from other functions. This allows an IT administrator to grant different employees or groups of employees access to different capabilities.

For example, an IT technician doing BIOS upgrades might need access to realms associated with general information (which gives firmware version information), redirection (remote boot/power-up), and firmware update capabilities. An IT technician monitoring PC health might need access only to the event manager.

Intel AMT supports multiple realms that can be assigned to any individual username(s). The following realms are available:

- Network and Intel AMT admin
- Event manager
- ISV storage admin
- ISV storage
- Hardware asset
- Redirection (IDE-R, or remote boot)
- Remote control (SOL, or console redirection)
- Local agent presence
- Remote agent presence
- Network outbreak containment (NOC)
- Firmware update
- Network time
- General info

The access-control lists for these realms are established during the configuration process.

Best practices

Best practices are also known as best known methods, or BKM. Refer to Appendix A for some recommendations of best practices for networking and security.

3PDS

Nonvolatile memory is divided into three areas. One of the areas – the 3PDS, or third-party data store – can be used by third-party vendors to write/store data specific to their applications. For example, a third-party vendor could store software version numbers, an update history, or configuration information in the 3PDS.

Terminology

- 3PDS – third-party data store
- ISV – independent software vendor
- MEI – management engine interface

Third-party data store (3PDS)

Intel AMT provides third-party applications with a mechanism to store data in nonvolatile memory. Controlled access to the data can be granted to other applications on the same device or from an authorized remote device. Intel AMT provides this capability through a set of commands that operate over a local host interface (the management-engine interface, or MEI) or through out-of-band communication over a network interface.

Third-party data-store (3PDS) is protected by control mechanisms which use the access control lists to enforce access to that space. ACLs are used to provide access to and permit allocation of nonvolatile memory for applications. Applications must register themselves with the Intel AMT-enabled device before they can use of the commands for accessing and managing the 3PDS.

The structure, meaning and sensitivity of data placed into the 3PDS are transparent to the 3PDS storage manager. As a result, applications are responsible for any security mechanisms necessary to protect their stored data (for example, they must encrypt their own sensitive data or keys).

Access control

Intel AMT uses access control lists (ACLs) to grant or revoke rights to particular capabilities, such as 3PDS or console redirection. This allows an IT administrator to grant different employees access to different capabilities. In general, best practices specify granting the fewest privileges necessary to any given user.

To gain access to a particular capability, IT technicians usually authenticate themselves first by logging into Intel AMT for a particular PC. Login is typically done using credentials such as a username and a password. The Intel AMT access-control mechanism then determines which realms the technician may access by comparing the user credentials to the ACL stored in tamper-resistant, nonvolatile memory.

The IT administrator usually defines the Intel AMT ACLs using a third-party application, such as a configuration service or a software management application (such as a management console). The ACLs are then loaded into Intel AMT via the configuration profile, during the configuration process. ACLs can also be loaded into Intel AMT via the management application.

Terminology

- FWSK – firmware signing keys

Firmware signing for Intel AMT firmware code

Intel signs the firmware code for Intel AMT using digital code signing technology. This ensures that the only firmware code executed by the Intel Management Engine is firmware code that is produced and digitally signed by Intel.

To provide end-to-end integrity and data-origin authentication for firmware images and manifests, a set of asymmetric firmware signing keys (FWSK) are generated and stored in the Intel Secure Facility (located in Oregon and California, USA). These keys are used to generate digital signatures for manifests. The public key that corresponds to the private key used to generate the manifest digital signature is placed in the manifest. Manifest digital signatures are generated using the RSA algorithm with modulus lengths of 2048 bits and public exponent values of 10001h (65537 decimal).

Intel AMT uses two unique FWSK key pairs at the same time: a primary key pair and a secondary key pair. The secondary key pair provides a backup key pair in case something happens to the primary key pair. For example, the secondary key pair can still be in place even if the primary key pair is compromised or destroyed.

A hash of the public portion of each FWSK is placed in the Intel AMT system ROM. This provides a root-of-trust embedded in the chipset hardware that can defeat flash-substitution attacks.

In addition, asymmetric keys are used to eliminate the need to create system or platform unique firmware images and manifests. Because only public keys (no secrets) are stored in the hardware for Intel AMT, the integrity and data-origin authentication protection mechanisms for firmware cannot be compromised by a hardware attack on any single PC with Intel AMT.

MEBx

The MEBx is the Intel Management Engine BIOS extension, which provides access to Intel AMT setup and configuration information, such as security credentials, networking mode, and other information.

PSK cipher suite used even without TLS

The PSK cipher suite can be used even for customers who do not have the certificate authority (CA) server required for general TLS use. This allows configuration to be performed securely, even if TLS is not enabled for use during normal device operations.

Terminology

- DHCP – dynamic host configuration protocol
- DNS – domain name server

Security during setup and configuration

For Intel AMT to be useful in corporations, it must be deployable into a wide variety of environments. These environments vary from large enterprises with trained IT staff who securely manage multisite networks, to small businesses with a few part-time technicians who manage a single-building network. Intel AMT is designed with a complete set of configuration and management functions to meet the deployment needs of administrators in each of these environments.

All setup and configuration processes are conducted using a combination of the BIOS-based Intel AMT configuration screen (MEBx) and the Intel AMT firmware, via communications over the network interface. Initial setup is typically done in a customer staging area by IT technicians. In some cases, the initial setup may be done by the OEM at the PC manufacturing site. In either scenario, Intel AMT must establish a secure link to the configuration server over the enterprise production network before configuration can be completed.

The protocol used for establishing a secure link between Intel AMT and the configuration server is the TLS protocol with preshared key (TLS-PSK) cipher suite. However, the PSK cipher suite can be used even if TLS is not enabled.

Operational or networking modes

To help Intel AMT operate in its destination environment, two operational modes are provided:

- **Enterprise mode,** for large enterprises that have a dedicated IT staff. This is an advanced setup mode that supports TLS and requires a setup application (the configuration service). It is the more secure setup and the recommended setup type.
- **Small-business mode,** for small businesses, or for enterprises that do not have DHCP and/or DNS available, or which do not use such services for security or other reasons. This is a simplified setup mode that does not support TLS, does not require a setup application, and is intended for environments that do not have a security infrastructure.

By default, Intel AMT is usually set to enterprise mode. However a PC manufacturer may preset the mode of operation to small-business mode when they build the PC. Authorized IT administrators can change this value later, through the MEBx screens, or through the network interface.

Secure configuration for enterprise mode, and basic configuration steps for small-business mode are described later in this section.

Establishing security credentials

In order to allow secure configuration of Intel AMT over the production network, the configuration communication has to be encrypted. This is achieved via the TLS preshared key (TLS-PSK) protocol.

Before third-party management software can access Intel AMT, the Intel AMT security credentials must also be set up, and security parameters must be configured for your IT environment. Setup is a prerequisite to the *CommitChanges* API call, which enables TLS.

Establishing security on the configuration server

To establish encrypted communication on the configuration server, you must add the administrator password, PID, and PPS to the server's tamper-resistant PSK repository. The configuration server must support:

- PSK information generation
- PSK storage for use by the configuration server
- PSK display, to allow entry into the PC with Intel AMT

For each PC to be deployed, you must:

1. Generate the 8-character provisioning ID (PID)
2. Generate a 32-character provisioning passphrase (PPS)
3. Add the password, PID, and PPS to the configuration server's tamper-resistant PSK repository

The information will be used to establish the initial, bootstrap security credentials for Intel AMT during setup.

Register configuration server as *ProvisionServer*

The configuration server should be registered in the enterprise DNS server as *ProvisionServer*. The hardware vendor can change this fixed name via the nonvolatile memory of Intel AMT. The configuration server is also called the CS server.

Best practices

Refer to Appendix A, Best Practices, for information about generating strong passwords and other security credentials

Establishing security
Setup establishes the initial security credentials for secure networking and TLS.

Configuration uses the security credentials to establish operational security – the link between Intel AMT and the configuration service.

Establishing security for Intel AMT

Establishing secure, encrypted communication for Intel AMT is a two-phase process that encompasses both the setup and configuration processes.

- **Phase I: set up security credentials.** This loads Intel AMT with the bootstrap security credentials required for encrypted networking and TLS. These credentials are required to activate the security capabilities of Intel AMT. Phase I consists of:
    1. Physically accessing the machine to power up the PC
    2. Entering the Intel AMT BIOS extension setup screens
    3. Changing the default factory password
    4. Entering the PID and PPS
    5. Programming the network settings as required for the enterprise environment
- **Phase II: establish operational security.** Security credentials are used to establish a secure link to the configuration server, so that the Intel AMT device can automatically complete its own configuration process. This process establishes operational TLS-PSK security for Intel AMT, including Kerberos settings, access control lists, and certificates and keys.

Phase I is the setup process for Intel AMT. Phase II is performed by the setup-and-configuration application, as part of the configuration process.

Three ways to set up Intel AMT

There are three ways to perform the setup process (phase I):

- IT automated method, in which an IT administrator uses a USB storage device to allow BIOS to load credentials into the PC. This is the most secure and least error-prone method of setting up Intel AMT.
- Manual method, by manually entering the information through the Intel AMT BIOS setup screen.
- OEM factory-automated method, in which factory tools are used to place credentials directly into flash ROM during manufacturing.

As soon as Intel AMT is set up with its initial security credentials, it is ready to be configured.

TLS-PSK details

The bootstrap credentials required for phase-I setup consist of a provisioning ID (PID) and a provisioning passphrase (PPS). The PID and PPS are covered with a cyclical redundancy check (CRC), to ensure that errors in manual entry are detected.

The PID and PPS are used to establish the TLS premaster secret. In compliance with the TLS-PSK RFC, the TLS premaster secret (PMS) is 68 octets long. Table 3-3 lists and briefly describes the TLS preshared key details for the bootstrap security credentials.

Table 3-3. TLS preshared key details

Key	Details
PID	64-bit quantity Consists of alphanumeric characters Case insensitive Example: *D64G-GXY6*
PPS	256-bit quantity Consists of alphanumeric characters Case insensitive Example: *MD97-QC74-TQJG-3V2W-27PV-RBDC-VTRC-D797*
PMS	68 octets in length

Secure enterprise-mode setup (TLS-secured)

The enterprise setup-and-configuration mode is designed to serve the needs of large enterprises that have an IT staff trained in securely managing multisite networks. When supported with the proper network infrastructure services, enterprise mode can provide automated, secure, “one-touch” configuration for Intel AMT devices.

Network requirements for secure setup

The area used for setting up Intel AMT should feature an isolated wired LAN with DHCP, DNS, and configuration servers. The wired LAN must be isolated from the rest of the enterprise network(s) to prevent disclosure of security-related parameters while they are being loaded into Intel AMT.

The configuration server should also support a secured connection over a second interface to a certificate-authority server. PCs in enterprise mode will typically have DHCP enabled by default.

Requirements for dynamic IP networking consist of:

- DHCP service
- DNS service
- Certificate authority service
- Configuration service, a third-party application that delivers operational settings to Intel AMT over the network. The CS completes the automated configuration process by supplying Intel AMT with customized parameters.
- Support for Microsoft Active Directory (optional). If you choose to use Kerberos security, you will need an environment that supports Active Directory.

Requirements for static IP networking consist of:

- Certificate authority service
- Configuration service, a third-party application that delivers operational settings to Intel AMT over the network. The configuration service completes the automated configuration process by supplying Intel AMT with customized parameters.
- Support for Microsoft Active Directory (optional). If you choose to use Kerberos security, you will need an environment that supports Active Directory.

Terminology

- CS – configuration service
- LAN – local-area network

Configuration service

The CS is a software service that performs all the necessary tasks to successfully configure Intel AMT, before they are put in use. The CS is provided by a third-party software vendor who supports the capabilities of Intel AMT in their software applications.

Manual setup and configuration when services are not available

If not all of the desired network infrastructure services are available in the isolated wired subnet (for example, a DHCP server is not available), enterprise networking can still be supported. However, you may be required to manually enter some of the data into Intel AMT.

Establishing certificates in staging area

An experienced IT administrator can set up an isolated staging environment that emulates the domains in which Intel AMT will be eventually used. For systems set up in this type of staging environment, Intel AMT could be fully set up and configured before PCs are delivered to the user desk.

During TLS-PSK setup:

- The digitally signed image is not changed
- Customization is to the data area only
- Passwords and PID-PPS pairs should be kept confidential
- When setup is performed by the PC hardware vendor, the IT administrator should replace passwords and PID-PPS pairs during in-house configuration.

Secure setup for networking and TLS

The first phase of establishing secure communication is performed via the setup procedure, which establishes the initial security credentials (refer to Figure 3-3 on the next page). This procedure follows these general steps:

1. **The CS generates PID and PPS.** The third-party CS generates a provisioning passphrase (PPS) and a provisioning ID (PID).
2. **The CS generates the premaster secret.** The CS generates a TLS premaster secret and stores the premaster secret in a database, along with other setup and configuration information (such as operational mode, TLS setting, and so on).
3. **The CS stores data for use during setup.** The CS stores the PPS, PID, new administrator password, and other configuration data in a USB storage device or provides it to the IT administrator in some other appropriate form.
4. **The IT administrator connects the PC.** The IT administrator unpacks the PC, connects it to a power source, and powers up the PC.
5. **The IT administrator updates BIOS and MEBx.** The IT administrator enters BIOS, enables the Intel Management Engine, and sets power policies for the management engine. The IT administrator then enters MEBx, activates Intel AMT, and enters the administrator password, PID, and PPS.
6. **The IT administrator exits MEBx.** The IT administrator exits MEBx, which causes the PC to reboot, and allows BIOS to finish loading upon the reboot.
7. **The IT administrator powers down the PC.**

This setup process can be automated via a USB device.

Once the setup procedure is completed, Intel AMT is set up with the appropriate keys, certificates, and other required data. The PC is then ready to be sent to the user and go through its self-initiated automated configuration, as described later in this guide.

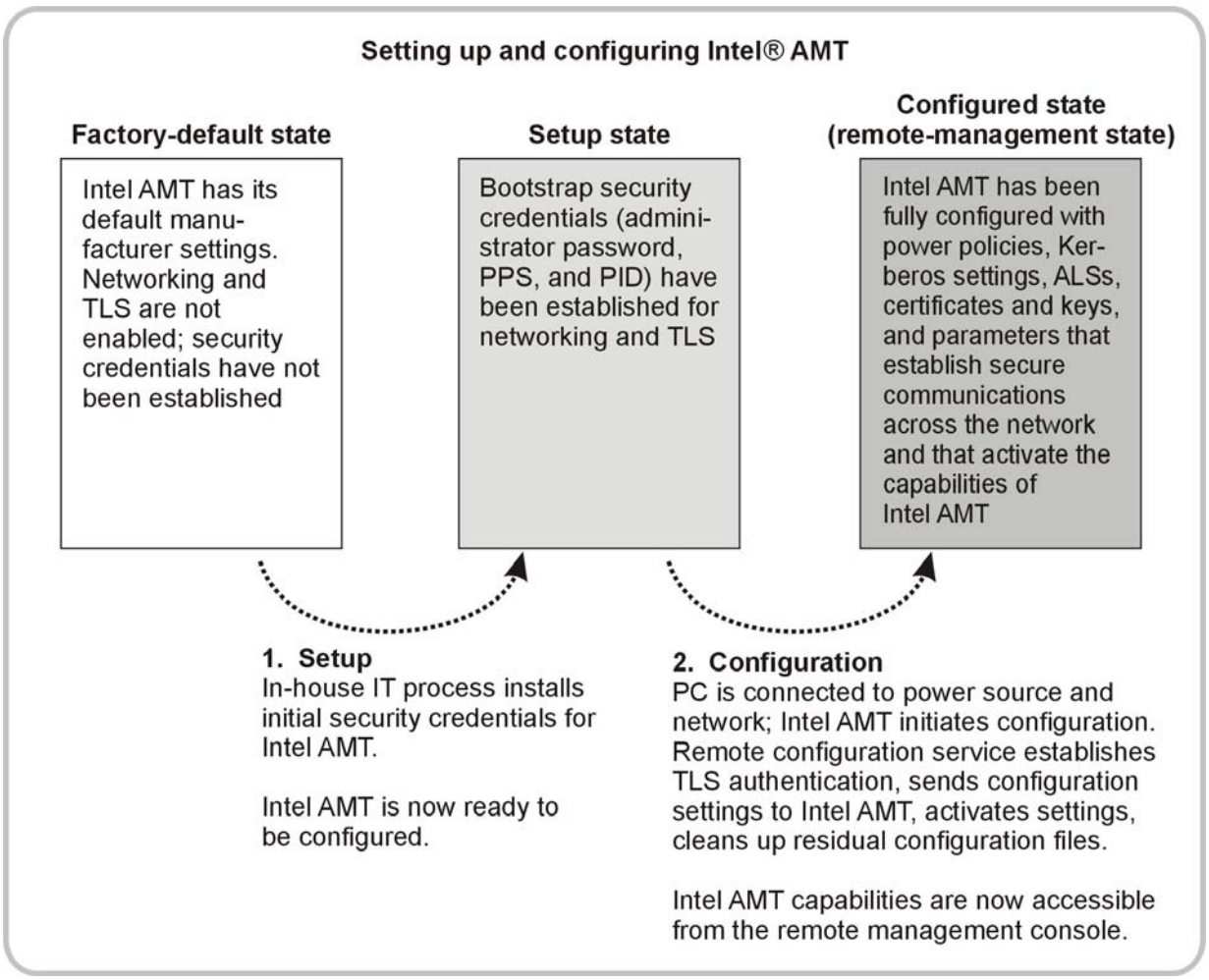

Figure 3-3. Setup and configuration of Intel AMT. Once Intel AMT is set up with its initial security credentials, automated configuration (including establishing certificates and keys) can be initiated by Intel AMT as soon as the PC is connected to a power source and plugged into the network.

Integrated TLS CA service

The TLS certificate authority service can be integrated into the CS.

Configuration: Establishing TLS-PSK security

The second phase of establishing secure communication is performed during the configuration process. This phase followed these general steps:

1. **The user connects the PC** to a power source and the network.
2. **Intel AMT locates the CS.** Intel AMT uses DHCP and DNS (or the networking parameters established during setup) to locate the CS.

3. **Intel AMT connects to the CS.** Intel AMT connects to the CS via a TCP/IP connection to the configuration service listening port 9971 (default).
4. **Intel AMT sends a hello packet.** Intel AMT sends a hello packet to the CS with its device-specific information: UUID, PID, IP address, ROM version numbers, and firmware version numbers
5. **The CS identifies the PC and its configuration profile.** The CS uses the PID from the hello packet to look up the TLS premaster secret in its database and locate the PPS associated with the PC.
6. **The CS establishes a secure TLS session.** The CS establishes a secure TLS session with the PC, using the PPS found in the repository, as per the TLS_PSK_WITH_AES_128_CBC_SHA cipher suite.
    - The CS generates the specific asymmetric keying material for the PC. This includes the TLS X509 certificate and the RSA private key.
    - The CS generates a TLS certificate request containing the RSA public key and the PC's fully qualified domain name (FQDN). The CS sends the request to the enterprise PKI system, and the enterprise PKI system returns a signed certificate to the CS.
    - The CS sends Intel AMT the trusted-root TLS certificate, a random number generator (RNG) seed, new PID and PPS values, and a new administrator password. The CS may also send a certificate revocation list (CRL).
7. **The CS logs into Intel Management Engine** using the Intel factory-default HTTP Digest network-administrator username and password.
8. **The CS loads Intel AMT with the configuration profile.** Using SOAP, the CS sends the appropriate configuration information to Intel AMT, including power policies, Kerberos settings, access control lists, the current date and time, HTTP digest credentials, HTTP negotiate credentials, and the information required to activate the capabilities of Intel AMT.
9. **The CS activates the settings.** The CS sends a reset command to the Intel Management Engine to activate the settings, clean up residual files, and complete the configuration process.

Once Intel AMT capabilities are fully configured, the PC is ready to be remotely managed by your third-party management solution.

TLS X509 certificate

The TLS X509 certificate contains the public key, UUID, networking domain name, and networking host name.

Automatic certificate generation

During automatic certificate generation, the TLS certificate authority service generates certificates and returns them in a certificate response to the CS.

For more information

Step-by-step processes for setting up and configuring Intel AMT devices are described in the quick-start section of this guide. Other sections provide background information on networking and configuration management.

Best practices (best known methods, or BKM) for networks and establishing security are provided in Appendix A of this guide.

Section 4
Setup and Configuration

Intel® AMT

Intel® Active Management Technology (Intel® AMT) is one aspect of the new hardware-based capabilities of Intel® vPro™ technology

Simple setup and configuration

The setup process for Intel AMT is relatively simple; and configuration, which is a self-initiated and automated process, typically takes only a few seconds.

Intel AMT and the PC

The setup and configuration processes described in this guide are not for the PC in general, but for Intel AMT. Intel AMT is one part of the powerful management engine built into PCs with Intel vPro technology.

Introduction

Networking and security can be complex areas that require significant expertise. Although deploying PCs with Intel AMT is fairly simple in itself, there are networking and security considerations that must be taken into account in your environment before secure communication can be established for the Intel AMT capabilities on the PC.

To help less experienced IT administrators, this section provides reference and background information on network and setup requirements, variations in network structures, Intel AMT configuration states, MEBx parameters, USB-key local provisioning, configuration profiles, and other setup and configuration considerations.

This section covers these topics:

- Overview of setup and configuration
- Deployment requirements
- Network components
- Establishing security credentials
- Enabling the Intel® Management Engine and Intel AMT
- Setting up Intel AMT
- Configuring Intel AMT
- Changing a host name or moving a PC
- Returning Intel AMT to its factory defaults

In environments where security is a high-priority concern, Intel recommends that PCs with Intel AMT be set up in-house, rather than by the PC hardware vendor.

Overview of setup and configuration

The deployment process for PCs with Intel AMT follows four general steps:

1. **Establish the management console,** including the configuration service.
2. **Generate unique key pairs** for each PC with Intel AMT.
3. **Set up Intel AMT** for networking and TLS by entering the administrator password, provisioning passphrase (the preshared key, or PPS), and provisioning ID (PID) into the PC. This sets up the initial, bootstrap security credentials required for secure network communication and for activating the capabilities of Intel AMT. Setup prepares Intel AMT to receive its configuration settings from a configuration service (CS).
4. **Configure Intel AMT** with security settings, power policies, and Intel AMT settings. This process specifies the power policies for the Intel Management Engine; and the Kerberos settings, access control lists, and certificates and keys for Intel AMT. This process also configures the PC with the settings that activate Intel AMT capabilities, including storage settings, event filters and subscriptions, filters and policies for the network outbreak containment capabilities, settings for agent-presence checking, and so on.

Setup is usually performed only once for each PC, and for security reasons, is usually performed in-house, by the IT administrator. This section includes background and reference information about both manual and semiautomated setup.

Once Intel AMT is set up, Intel AMT is ready to initiate configuration of its own capabilities. When all required network elements are available, this can be a fully automated configuration process. The user simply connects the PC to a power source and the network, and Intel AMT automatically initiates its own configuration. The configuration service (CS), a third-party application, completes the process for you. Intel AMT is then ready for remote management. Automated configuration typically takes only a few seconds.

Once Intel AMT is setup and configured, the technology can be reconfigured as needed for your business environment. Refer to the configuration management section for information about unconfiguring and reconfiguring Intel AMT after security credentials (setup) have been established.

Terminology

- CS – configuration service
- MAC – media access controller
- MEBx – management engine BIOS extension
- PID – provisioning ID
- PPS – provisioning passphrase (the preshared key required for TLS)
- PSK – preshared key

Preprovisioning and provisioning

The setup process is sometimes called “preprovisioning” the PC. The configuration process is sometimes called “provisioning” the PC.

Security considerations

In environments in which security is a high-priority concern, Intel recommends that you perform the setup procedure in-house to establish the initial, bootstrap security credentials.

Security credentials

The information required to establish the initial, bootstrap networking and TLS security credentials consists of the administrator password, provisioning passphrase (PPS), and provisioning ID (PID).

Configuration profile

A file containing power policies, Kerberos settings, access control lists, certificates and keys, and the settings that activate Intel AMT.

Three setup and configuration states

There are three setup and configuration states for Intel AMT:

- **Factory-default state.** A fully unconfigured state, in which security credentials are not yet established, and Intel AMT capabilities are not yet available to management applications. In the factory-default state, Intel AMT has the factory-defined settings.
- **Setup state.** A partially configured state, in which Intel AMT has been set up with initial networking and TLS information: an initial administrator password, the provisioning passphrase (preshared key, or PPS), and the provisioning identifier (PID). When Intel AMT has been set up, Intel AMT is ready to receive enterprise configuration settings from a configuration service (CS).
- **Configured state.** A fully configured state, in which the Intel Management Engine has been configured with power policies, and Intel AMT has been configured with its security settings and certificates, and the settings that activate the Intel AMT capabilities. When Intel AMT has been configured, the capabilities are ready to interact with management applications.

Figure 4-1 shows the general setup and configuration states for deploying Intel AMT.

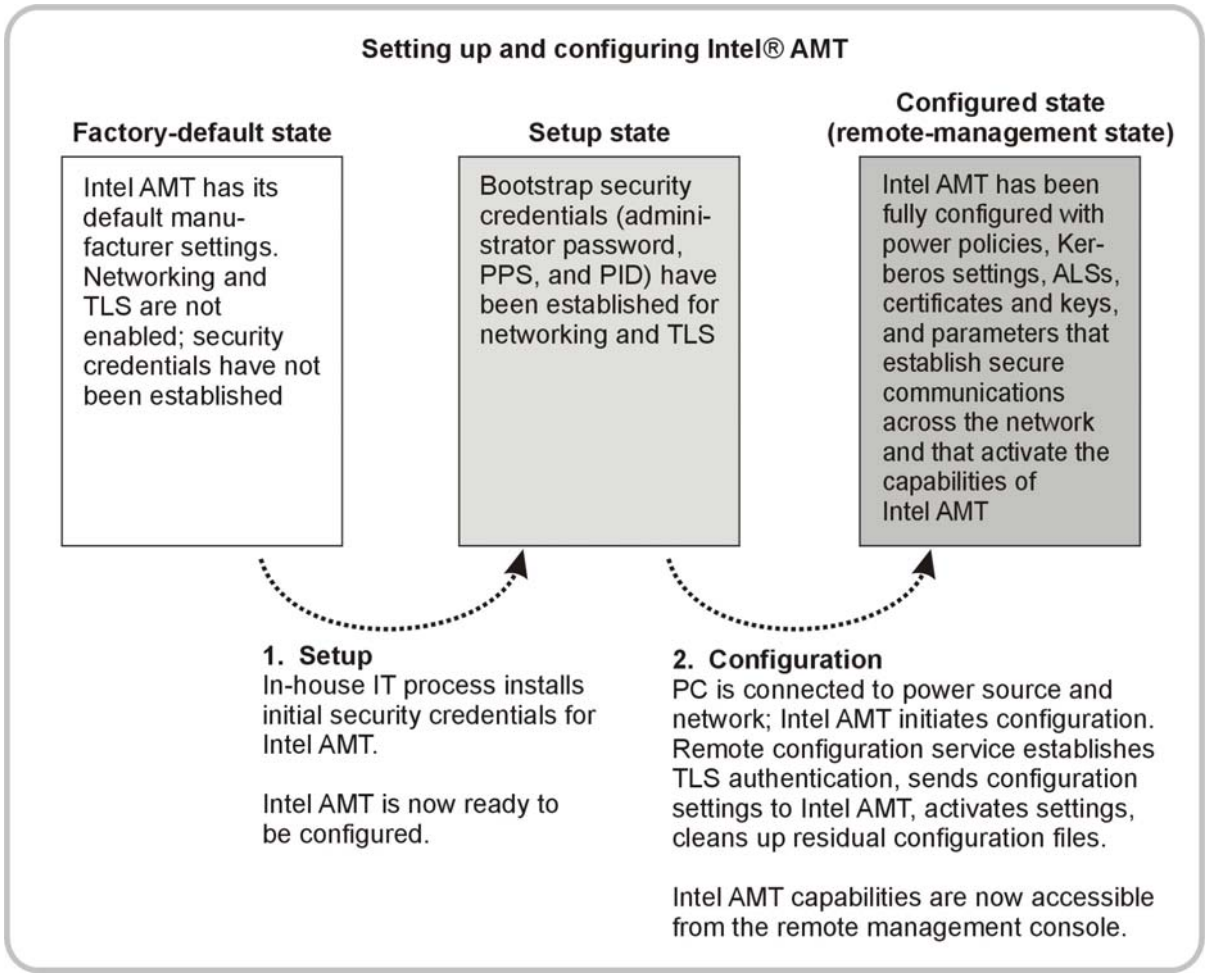

Figure 4-1. Configuration states. Once Intel AMT is set up and configured, the capabilities are accessible to the remote management console.

When PCs arrive at the customer site

PCs arrive in at the customer site with Intel AMT in one of two states: factory-default state (preferred for security reasons), and setup state.

- **When Intel AMT is in factory-default state,** the IT administrator performs the Intel AMT setup in-house.
- **When Intel AMT is already set up,** it is already set up by the OEM factory and ready for automated configuration at the customer site**.**

In-house setup can be done through a semiautomated process via a USB flash device. In-house setup can also be performed by manually entering the information required for establishing the initial security credentials via the BIOS extension screen. OEM setup is performed at the PC vendor's factory.

Automated vs. manual setup

You can set up Intel AMT in different ways, depending on the amount of automation available to you in your manufacturing or network environment:

- Automated setup, in which you use a USB storage device to load credentials into each PC.
- Manual setup, in which you manually enter the information through the BIOS extension screen.
- OEM factory-automated setup, in which your hardware vendor uses factory tools to place credentials directly into flash ROM during manufacturing.

The most secure method of establishing security credentials is in-house IT setup. For security reasons, Intel recommends that you establish the security credentials for your business, rather than accept OEM-defined setup credentials.

Enterprises using small-business mode

In some cases, an enterprise might not want to use DHCP networking or DNS. In these cases, IT administrators can still set up and configure Intel AMT in enterprise mode, by manually supplying a static IP address during the configuration process. The IT administrator can also use small-business mode instead of enterprise mode, to configure Intel AMT for environments that do not have DHCP or DNS.

Changing the operational mode

Intel AMT must be in the setup state in order for you to be able to change the operational mode (enterprise or small-business). If Intel AMT is already configured, you must unconfigure Intel AMT to return it to the setup state before you can change the operational mode.

Two operational modes

Intel AMT can be set up for either enterprise or small-business operations (also called provisioning models). Both operational modes support dynamic- and static IP networking. The PC vendor specifies the default operational type when building the Intel vPro technology (which includes Intel AMT) flash image.

- **Enterprise mode,** for large organizations that have a dedicated IT staff. This is an advanced networking mode that supports TLS and requires a configuration service. Enterprise mode allows IT administrators to set up and configure Intel AMT in a secure manner for remote management. Enterprise mode is the recommended operational mode.
- **Small-business mode,** a simplified operational mode that does not support TLS, does not require a setup application, and does not require DHCP or DNS.

The primary difference between enterprise mode and small-business mode is support for TLS. Small-business mode is appropriate for businesses that do not have the IT infrastructure to support an enterprise setup with TLS, or which do not use DHCP or DNS for security reasons.

The second key difference is that, in small-business mode, after being setup, Intel AMT will not automatically try to look for a configuration server or send its hello packets. However, once Intel AMT is set up, you could use a third-party software application to perform remote discovery and automatic configuration in the small-business model.

If you are an IT administrator deploying PCs for a small- or medium- business (SMB) site, refer to the appropriate small-business setup and configuration manual for information about how to setup and configure Intel AMT for small-business environments.

This guide describes enterprise operational mode setup and configuration for both dynamic IP and static IP networking environments.

Terminology

- MAC – media access controller

MAC addresses

In dynamic IP networking, the same IP address is used for both the host and Intel AMT.

In static IP networking, Intel AMT requires a fixed IP address separate from the host OS, and uses a separate manageability MAC address.

Dynamic vs. static IP environments

Intel AMT-enabled PCs can be configured for dynamic (DHCP) or static IP environments. To allow you to choose the networking mode that best suits your environment, hardware vendors configure the PCs with two MAC addresses:

- MAC address for the host (the PC's operating system)
- Manageability MAC address for the Intel Management Engine

The IP address for Intel AMT (which is part of the Intel Management Engine) is specified during setup of Intel AMT.

Dynamic IP (DHCP) environments

Typically, OEMs set up Intel AMT to use dynamic IP networking by default, via DHCP and DNS. In dynamic IP networking, the same IP address is used for both the host (the PC's operating system) and Intel AMT. The firmware stack in Intel AMT looks at the communication port to differentiate communication with Intel AMT from communication with the OS.

Intel AMT conforms its settings to the PC's operating-system (the host) network settings.

Intel AMT uses DHCP option 81 to register the PC's host name in the DNS server. This is required because the host name is embedded in the TLS certificate. The configuration server (or later, the remote management console or third-party management application) retrieves the host name from DNS for comparison before authenticating communication with Intel AMT.

Static IP environments

In static IP environments, the PC has fixed network settings. In these environments, Intel AMT requires a fixed IP address and uses a separate manageability MAC address. To let you choose a static IP environment (and define a static IP address for Intel AMT), hardware vendors configure Intel AMT-enabled PCs to have two MAC addresses:

- MAC address for the host (the PC's operating system)
- Manageability MAC address for the Intel Management Engine

During setup, you must manually enter the static (dedicated) IP address for Intel AMT in each PC.

Deployment requirements

The staging area which your IT organization uses to set up Intel AMT must include certain network and configuration equipment, services, and applications for secure setup and configuration.

Personnel requirements

Before deploying Intel AMT devices, make sure your IT personnel have adequate training and experience. Deployment personnel should be experienced in:

- System administration
- Security methodologies and technologies, including transport layer security (TLS), secure sockets layer (SSL), and preshared key infrastructures (PKI)
- IT management tools and consoles

Intel offers training in best known methods (BKM) for deploying systems in an enterprise environment. Intel can also provide you with a list of authorized dealers and channel service providers who are experienced in deploying Intel AMT.

Training

For information about training, contact your Intel account team or local sales office.

Network and setup requirements

Network and application requirements are different for dynamic IP and static IP networking. Table 4-1 lists the network and application requirements for setting up and configuring Intel AMT.

Table 4-1. Setup and configuration requirements

Network element	Dynamic IP	Static IP
DHCP service	Required	–
DNS service	Required	Optional[1]
Certificate authority service	Required	Required
Configuration service	Required	Required
Support for Microsoft Active Directory*	Optional[1]	Optional[1]

[1] If you choose to use Kerberos security, you will need an environment that supports Microsoft Active Directory.

Dynamic IP

DHCP is often called dynamic IP.

DHCP service

If you are deploying Intel AMT-enabled PCs for dynamic IP networking, make sure your infrastructure supports the minimum requirements for DHCP networking.

* Other names and brands may be claimed as the property of others.

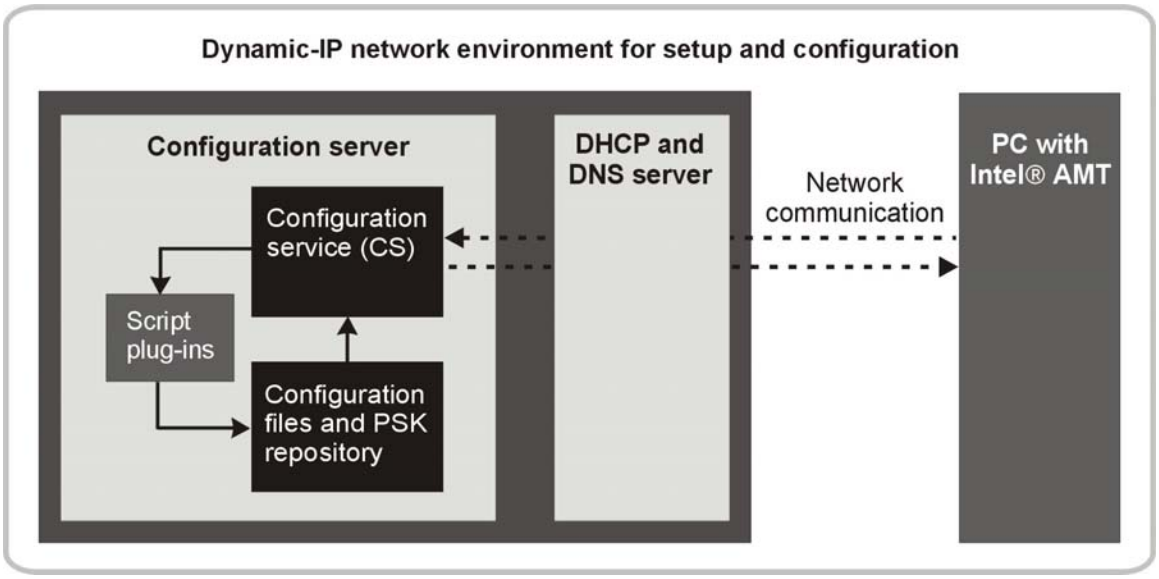

Figure 4-2. Network configuration for dynamic IP with TLS.
DHCP and DNS are required in dynamic IP networking.

OEM-defined level of integration

The OEM and/or third-party management-software vendor can choose the level of integration used between the configuration server, certificate authority server, and/or a directory-based management server, such as Active Directory.

Requirements for dynamic IP networking with TLS

Networking requirements for dynamic IP consist of:

- DHCP service
- DNS service
- Certificate authority service
- Configuration service (CS), a third-party application that delivers operational settings to Intel AMT over the network. The CS completes the automated configuration process by supplying Intel AMT with customized parameters.
- Support for Microsoft Active Directory (optional). If you choose to use Kerberos security, you will need an environment that supports Active Directory.

Figure 4-2 (above) shows the network components and their interactions for dynamic IP networking with TLS.

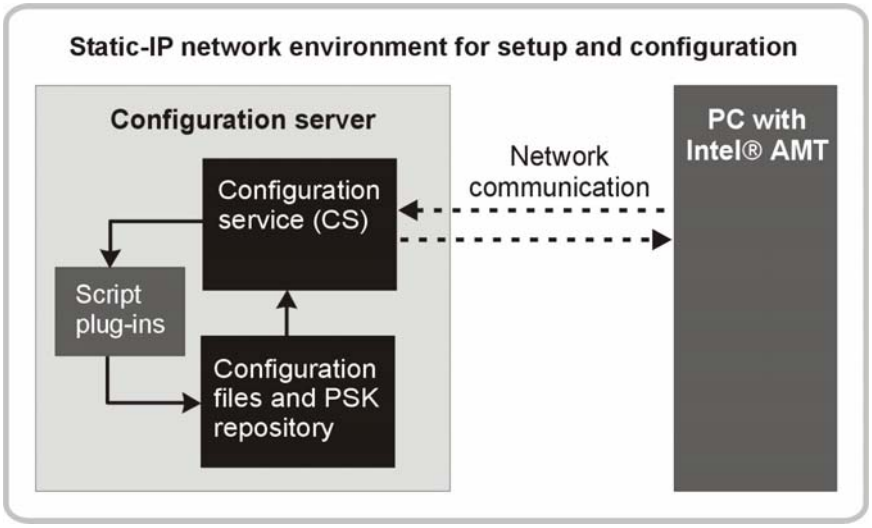

Figure 4-3. Network configuration for static IP with TLS. DHCP and DNS are not required in static IP networking.

Requirements for static IP networking with TLS

Networking requirements for static IP consist of:

- Certificate authority service
- Configuration service (CS), a third-party application that delivers operational settings to Intel AMT over the network. The CS completes the automated configuration process by supplying Intel AMT with customized parameters.
- Support for Microsoft Active Directory (optional). If you choose to use Kerberos security, you will need an environment that supports Active Directory.

Figure 4-3 (above) shows the network environment for static IP networking.

Terminology

The configuration server is also called the CS server (configuration-service server) or the provisioning server.

The certificate authority server is also called the CA server.

DHCP and DNS not available

If DHCP and DNS are not available in your environment, Intel AMT cannot use those services to automatically locate the configuration server to initiate its own configuration process. Instead, you must usually disable those default settings. You must then enter the appropriate IP address of the configuration server in the MEBx.

Changing certificates

The certificate is permanent as long as the PC remains in its location, the host (the PC operating system) name remains the same, and the domain name remains unchanged. Those settings are part of the certificate. If those settings change, a new certificate must be generated for Intel AMT.

Network components

This discussion briefly describes the network components required for dynamic IP or static IP networking.

DHCP server

When setup is properly completed, Intel AMT automatically tries to obtain its own networking settings as soon as the PC is connected to a power source and plugged into the network. The PC manufacturer typically specifies that, by default, Intel AMT will try to obtain its networking settings from a DHCP server.

If DHCP services are not available, Intel AMT must be configured to use static IP networking. The quick-start section of this guide explains how to set up Intel AMT for static IP networking.

DNS server

When Intel AMT begins its configuration process, it automatically tries to locate the configuration service. OEMs typically specify that, by default, Intel AMT tries to obtain the IP address of the CS server by performing a DNS query for a host name *ProvisionServer*.

Keep these considerations in mind when using a DNS service:

- If DNS is enabled and a DNS server is unavailable, or if Intel AMT is unable to resolve the host name, setup and configuration will fail.
- If DNS is not available for your network environment, you must enter the IP address of the CS server in the MEBx screens during setup.

The quick-start section of this guide explains how to specify the IP address of the CS server during setup.

Certificate-authority server

TLS requires that each Intel AMT-enabled PC has a signed certificate that is traceable to a certificate authority. The certificate-authority (CA) server is the network element that creates the certificate. During communication with Intel AMT, the CA validates the certificates for the server (Intel AMT on the PC) and client (the configuration service).

Configuration service

The configuration service (CS) is a third-party software service, such as an application or a management console, that performs the tasks necessary to successfully setup and configure Intel AMT before Intel AMT is put in use.

Basically, the configuration service implements the request, signing, and installation of a server certificate in an Intel AMT-enabled PC. The configuration service then delivers the operational settings for the Intel AMT capabilities (customized for your environment) to Intel AMT over the network. The configuration service is provided by a third-party software vendor who supports Intel AMT in the vendor's software applications.

Provisioning server

The CS is run on a configuration server, which is sometimes referred to as a provisioning server.

Configure and initialize the CS

The configuration service must be set up to correctly configure Intel AMT for its operational environment, and so that communication with Intel AMT is encrypted and secure. The mutual authentication capability of Intel AMT requires that appropriate certificates and keys be established in both Intel AMT and in the CS server before configuration begins.

CS must have access to PSK repository

The PID-PPS pair for each PC is stored in the PSK repository of the configuration service. The keys are required for secure, encrypted communication with Intel AMT during configuration. Make sure the PSK repository is available to the configuration service before beginning configuration of Intel AMT.

In general, configuring the CS includes:

1. Setting up the application to conduct certificate operations.
2. Defining the preshared key (PSK) repository for the PCs.
3. Setting up a configuration *.xml* file(s) that contains the general configuration settings that will be applied to the Intel AMT capabilities on the PCs.

Refer to your third-party's configuration-service documentation for detailed information about setting up your configuration service.

CS not typically available to Intel AMT during setup

In a typical deployment, the configuration service is not available to Intel AMT until after the PCs have been moved to their working location, such as the user desk. This is because IP address, time-date, and other user-location information are used to establish the TLS certificate and help prevent malicious man-in-the-middle attacks.

Once set up, Intel AMT automatically tries to configure itself as soon as it is connected to a power source and the network. This includes establishing its unique security certificates with the settings loaded by the configuration service: current IP address, domain name, time and date stamp, and other user-specific settings.

Establishing certificates in the staging area

An experienced IT administrator can set up an isolated staging environment that emulates the domains in which Intel AMT will be eventually used. For systems set up in this type of staging environment, Intel AMT could be fully set up and configured before the PCs are delivered to the user desk.

Basically, when MEBx setup is complete and BIOS finishes loading, Intel AMT automatically begins sending hello packets to the configuration service. This begins the automated configuration process, in which Intel AMT will try to initiate its own configuration, and the configuration service will try to complete this process for you.

- **If the CS is available** in the staging area, then as soon as BIOS finishes loading (at the end of the setup procedure), Intel AMT will configure its networking information and security certificates for use in that domain.
- **If the CS is not available** until after the PC has been plugged in to power and the network at the user desk, then Intel AMT will establish its TLS certificate for the user location.

Most IT administrators will move the PC to the user desk, and make the configuration service available to Intel AMT in that domain. However, an experienced IT administrator could set up an isolated staging environment that emulates the domains in which Intel AMT will be used. This would include emulating the IP address, time-date stamp, and other unique information for the user's domain. In this scenario, Intel AMT could be fully set up and configured before the PCs are delivered to the user desk. This can be a useful process in environments in which security is a high priority.

Web interface API

By default, the Web interface is disabled for enterprise mode. However, an API that enables the interface for enterprise mode is available to management-console vendors.

Changing operational type

The operational type – enterprise or small business – can be changed only when Intel AMT is in factory mode. Restoring Intel AMT settings to factory mode is done through the MEBx screen or over the network using the SOAP interface (refer to the configuration management section of this guide).

Register configuration server as *ProvisionServer*

The configuration server should be registered in the enterprise DNS server as *ProvisionServer*. Upon request by the customer, the hardware vendor can change this fixed name.

Configuration tools

There are two types of configuration-interface tools available for configuring Intel AMT: the third-party configuration API (application programming interface) and a Web interface.

- **Configuration API,** a third-party software application that authenticates Intel AMT, loads configuration information into Intel AMT, reboots the PC to activate the Intel AMT settings, and cleans up residual files. You can use a configuration API in enterprise mode or small-business mode.
- **Web interface** network settings page, available only in small-business mode. The Web interface is enabled when the provisioning model is set to small-business during the setup procedure. The Web interface lets you:
  - Change the administrator password
  - Set up the network configuration
  - Define access control lists for the realms associated with the capabilities of Intel AMT
  - Access hardware-asset inventory and event log
  - Perform some remote-control capabilities

The next discussion provides background and reference information about security for both dynamic IP and static IP environments.

Security during setup and configuration

In order to allow secure configuration over the production network, the configuration communication to Intel AMT must be encrypted. This is achieved via the TLS preshared key (TLS-PSK) protocol, as described in the security section of this guide.

Before third-party management software can access the Intel AMT capabilities, the initial security credentials must be set up, and security parameters configured for your IT environment. Setup is a prerequisite to the *CommitChanges* API call, which enables TLS.

Once Intel AMT is set up and the PC is moved to its working location, certificates must be established for both the server (Intel AMT) and the client (the configuration service). Once both server and client have been authenticated, automated configuration can be performed.

Security in the staging area

During setup, Intel AMT is populated with an administrator password, PPS, and PID, which are necessary for encrypted communications and to activate the Intel AMT capabilities. In environments where security is a high-priority, Intel recommends that you set up the initial security credentials in-house.

Establishing certificates in staging area

An experienced IT administrator can set up an isolated staging environment to fully set up and configure Intel AMT before PCs are delivered to the user desk. This can be useful in environments in which security is a high priority.

The staging area for Intel AMT setup should feature an isolated wired LAN (local area network) with DHCP, DNS, and configuration servers. The wired LAN must be isolated from the rest of the enterprise network(s) to prevent disclosure of security-related parameters while that information is being loaded into Intel AMT.

Caution

Intel AMT should be configured on an isolated network during initial setup, in order to minimize exposure of sensitive information, such as passwords. During initial setup and before TLS certificates and keys are configured, the configuration traffic is sent without encryption. Once TLS authentication is in place, typical security procedures can be applied.

Note

If the configuration server requires access to both a user network and the isolated configuration network, equip the server with more than one network interface. You can then use one network device to establish isolated network connections to the Intel AMT-enabled systems to be configured. You can use the second network device to connect to the user network.

The configuration server should also support a secured connection over a second interface to a certificate authority server. DHCP is usually enabled by default in PCs with Intel AMT.

Establishing security on the configuration server

The configuration server must be set up to meet enterprise security requirements, not just the deployment requirements for configuring Intel AMT. For example, when TLS is used for secure communications, the configuration server must support mutual authentication. If the configuration service is a separate application from the management console, both the management console and the configuration service must have individual certificates.

To establish encrypted communication on the configuration server, you must add the administrator password, PID, and PPS to the server's secure PSK repository. The configuration server can provide you with a copy of these parameters on a USB storage device.

Verify access to the PSK repository

The PID-PPS pair for each PC is stored in the PSK repository of the configuration server. The keys are required for secure, encrypted communication with Intel AMT during configuration. Make sure the PSK repository is available to the configuration server before beginning Intel AMT configuration.

The configuration server must support:

- PSK information generation
- PSK storage for use by the configuration server
- PSK display, to allow entry into Intel AMT on the PC.

For each PC being deployed, you must:

1. Generate the 8-character provisioning ID (PID).
2. Generate a 32-character provisioning passphrase (PPS).
3. Add the administrator password, PID, and PPS to the configuration server's secure PSK repository.

Establishing secure communications to Intel AMT

Establishing secure, encrypted communication to Intel AMT is a two-phase process:

- **Phase I: set up security credentials.** This loads Intel AMT with the bootstrap security credentials required for networking and TLS. These credentials are required to activate the security capabilities of Intel AMT. To set up the initial security credentials, you must:
    1. Physically access the machine to power up the PC.
    2. Enter the Intel AMT BIOS extension setup screens.
    3. Change the default factory password.
    4. Enter the PID and PPS.
    5. If necessary, program the network settings as required for the enterprise environment.
- **Phase II: establish operational security.** Security credentials are used to establish a secure link to the configuration server. This is usually initiated by Intel AMT, completed by the CS, invisible to the user, and performed automatically. The process establishes operational TLS-PSK security for Intel AMT, including Kerberos settings, access control lists, and certificates and keys.

Phase I is the setup process. Phase II is performed by the CS, as part of the configuration process. (These procedures are described in the quick-start section of this guide.)

In general, you can start the setup process as soon as the Intel Management Engine and Intel AMT are enabled. The management engine and Intel AMT are typically enabled by default.

Enable Intel® Management Engine and Intel® Active Management Technology

The Intel Management Engine must be enabled in BIOS in order for you to access the MEBx screens. Within MEBx, Intel AMT must also be enabled in order for you to setup and configure Intel AMT. Typically, both the management engine and Intel AMT are disabled by default in PCs that arrive from the factory.

Sleep states and availability of Intel AMT

Intel AMT capabilities are available to the remote management console based on the sleep states specified for the Intel Management Engine power policies. For example, if the management engine is available in sleep state S5, the management engine can communicate with the remote management console even when the PC is powered off. When the management engine is available in S1 through S5, the Intel AMT capabilities are available in any sleep state, including hibernate and powered-off states.

Power policies for the Intel Management Engine are loaded into the PC during configuration, as part of the configuration profile. Depending on the OEM configuration of the PCs, when you first receive the systems, it may be necessary to power up the PC in order to wake the management engine for configuration. This would allow Intel AMT to initiate the automated configuration and update its own power policies.

Waking the management engine

PCs with Intel AMT are enabled for out-of-band communication. They do not necessarily have to be powered up in order to establish a connection to a configuration server, or to perform the self-initiated and automatic configuration process. At the customer's request, the PC manufacturer can allow the Intel Management Engine to be on for first application of power.

Setup

You can verify and/or update the power policies for the Intel Management Engine during setup. The quick-start section describes setup procedures.

Waking the management engine

Configuration of Intel AMT begins when the CS (configuration service) receives a hello packet from Intel AMT. Configuration itself depends on Initialization of the hello packet; basically, *when* the hello packet can be sent by Intel AMT. In turn, that depends on the power policies set up for the Intel Management Engine.

When the management engine is available in any sleep state, the Intel AMT hello packets can be sent as soon as the system is connected to power and plugged into the network. At the customer's request, the PC manufacturer can allow the Intel Management Engine to be on for first application of power. This would allow Intel AMT to send hello packets as soon as the PC is connected to a power source and the network, even if the PC itself is powered off.

However, some manufacturers might ship PCs with the management engine off for Sx (sleep states S1 through S5), in order to comply with more stringent energy requirements. If power policies are set to disable the management engine in sleep states S1 through S5, the hello packets will not be sent until the PC is first powered on.

Depending on the OEM configuration of the PC, it may be necessary to power up the PC in order to wake the management engine and allow Intel AMT to initiate its automated configuration process. You can use the MEBx screens to set the power policies for the management engine during the setup procedure.

Enable ME throughout the BIOS

Make sure you have enabled the Intel Management Engine throughout the BIOS. For example, if your BIOS manufacturer separates the chipset from the I/O controller hub (ICH), you might need to enable the management engine in both the main chipset and in the ICH fields.

Power policies for management engine

If you want Intel AMT to automatically configure itself as soon as the PC is connected to power and plugged into the network, the management engine should be enabled for sleep states S1 through S5.

Verify management engine and Intel AMT settings

Some IT administrators prefer to verify the status of all required settings for a technology during setup and configuration. This discussion explains how to verify and/or change the status of the Intel Management Engine and Intel AMT settings. Because BIOS and MEBx settings are vendor-dependent, the verification procedure describes general steps.

Follow these general steps to verify and, if necessary, change the status of the BIOS and MEBx settings for the Intel Management Engine and Intel AMT:

1. In BIOS, make sure the Intel Management Engine is enabled.

   Make sure you enable the management engine throughout the BIOS. For example:

   - Enable the management engine in the Northbridge main chipset (the main CPU).
   - Enable the management engine in the Southbridge chipset (the ICH, or I/O controller hub).

2. Enter MEBx.
3. When prompted, enter the administrator password.
4. Select the configuration screen for management-engine features.
5. Verify that the manageability mode is set to Intel AMT, or change the mode to Intel AMT.
6. Using the power-control feature, make sure the Intel Management Engine power policies are set to your operational preference.

   Caution:

   Changing the manageability mode will fully unprovision Intel AMT – erasing the configuration profile and the initial security credentials for Intel AMT – and return Intel AMT to its factory-default state. To gain remote access to the Intel AMT capabilities again, you must follow the setup and configuration processes.

7. Exit MEBx.

The PC will then automatically reboot.

Once the Intel Management Engine and Intel AMT are enabled, you can access the MEBx screens, perform the setup procedure, and allow automatic configuration to occur.

If you are enabling the management engine, setting power policies, and enabling Intel AMT as part of the setup procedure, you would typically make the rest of the MEBx changes before exiting MEBx and allowing the system to reboot.

Delayed deployment of Intel AMT

Delayed deployment

In a typical delayed deployment, security credentials for Intel AMT might be set up, but would not be allowed to configure itself. In this case, you could still perform remote configuration once the hello packet sequence is reinitialized.

In some IT environments, PCs with Intel AMT will be deployed and in use without the remote management capabilities of Intel AMT being configured (Intel AMT is not configured to its operational mode). In these environments, the IT administrator might set up the security credentials for Intel AMT as the PCs arrive at the corporation, but might not make the configuration service available to Intel AMT. This would leave the Intel AMT capabilities in an unconfigured state, so that the capabilities were not available across the network.

When you later want to configure Intel AMT to make those capabilities available to the remote management console, you may have to reinitialize the hello-packet sequence. This would allow Intel AMT to initiate its automatic configuration. Depending on your PC configuration, you might also have to reset the manageability mode to Intel AMT.

Reinitializing the hello packet sequence and changing the manageability mode are described next.

Reinitializing the hello packet sequence

Hello packets

Refer to the discussion “Hello packet,” later in this section, for information about the hello packet sequence.

When Intel AMT has been set up, but the configuration service is not available, Intel AMT still sends its hello packets at predefined intervals to continue trying to initiate configuration. The interval for sending hello packets will increase the longer there is no response from the CS. After some time (days or weeks), the interval will be long enough that it might appear that the hello packets have expired and the Intel AMT capabilities are inactive. To configure Intel AMT after a delayed deployment of the PC, you might need to reinitialize the hello packet sequence.

The steps for reinitializing the hello packet sequence depend on the power policies defined for the Intel Management Engine. During setup, you should make sure the power policies for the management engine are set so that you do not have to disconnect and reconnect PC power in order to reinitialize the management engine.

There are two ways to reinitialize the hello packet sequence:

- If the Intel Management Engine is configured to reinitialize upon a power cycling, you can power down and power up the PC (cold reboot) to reinitialize the hello packet sequence. Typically, if your network environment allows it, you would use your third-party management console to power down the PC and power the system back up to reinitialize the hello packet sequence.
- If the Intel Management Engine is not configured to reinitialize upon a power cycling, you will probably have to disconnect the PC's power source (for example, unplug the PC from its power source), reconnect power, and power up the PC again in order to reinitialize the hello packet sequence.

Once the hello packet sequence is reinitialized, Intel AMT can begin sending hello packets to begin its self-initiated, automated configuration.

Changing the manageability mode

Changing manageability mode

Changing manageability mode (for example, to ASF) will automatically return Intel AMT to its factory-default state. To enable Intel AMT from the factory-default state, you must follow the setup and configuration processes described in the quick-start section of this guide.

In environments in which PCs have been in use for some time before the Intel AMT capabilities are configured, the manageability mode in MEBx might not be set to Intel AMT. For example, the manageability mode in such an environment might be set to ASF (alert standard format).

In order for Intel AMT capabilities to be configured and available for remote management, the manageability mode must be set to Intel AMT.

Caution:

Changing the manageability mode will return Intel AMT to its factory defaults, erasing the configuration profile and the initial security credentials for Intel AMT. To gain remote access to the Intel AMT capabilities again, you must follow the setup and configuration processes.

Note:

In environments in which security is a high-priority concern, setup should be a manual process.

Changing the manageability mode is typically done through MEBx during setup of Intel AMT. Refer to the procedure under "Verify management engine and Intel AMT settings," earlier in this section, for the general steps to change the manageability mode.

Terminology

- MEBx – the management engine BIOS extension
- PID = provisioning ID
- PPS = provisioning passphrase (the preshared key required for TLS)
- PSK – preshared key

Setup using MEBx

The MEBx is the management engine BIOS extension. The BIOS extension specifies the networking parameters, security settings, and settings that activate or disable specific Intel AMT capabilities. This discussion describes common settings you might specify or change during setup and/or configuration.

Access to BIOS and MEBx and access to the parameters you can change is dependent on your hardware vendor's implementation.

Factory-default settings

Your hardware vendor should have set several BIOS settings to default values appropriate for your network. Typically, the provisioning mode is enterprise, TLS is enabled, and DHCP is enabled. If you are using the default enterprise settings (recommended), the setup procedure typically requires changing only three values in BIOS and MEBx, and entering a unique administrator username-password, PID, and PPS.

Table 4-2 lists the typical default BIOS and MEBx settings and the values of those settings after setup.

Table 4-2. BIOS and MEBx settings

BIOS or MEBx setting	Typical default	Value after setup
Intel Management Engine	Disabled	Enabled[1]
Sleep-state power policies for Intel Management Engine	Off	On for S1-S5[2]
Intel AMT	Disabled	Enabled[1]
Provisioning mode	Enterprise	Enterprise
TLS	Enabled	Enabled
DHCP	Enabled	Enabled for dynamic IP networking Disabled for static IP networking

[1] The Intel Management Engine and Intel AMT must be enabled in order for you to set up, configure, and use Intel AMT.

[2] Setting power policies for the management engine to S1 - S5 allows Intel AMT to initiate configuration in any power state, as soon as the PC is connected to power and plugged into the network.

DHCP and DNS not available

If DHCP and DNS are not available in your environment, Intel AMT cannot use those services to automatically locate the configuration server to initiate its own configuration process. Instead, you must usually disable those default network settings. You must then enter the appropriate IP address of the configuration server in each PC's MEBx.

Entering BIOS is vendor-dependent

During power up, the PC will first display the BIOS startup screen, then process the BIOS extensions. The specific steps for entering BIOS will depend on your hardware vendor.

MEBx settings are vendor-dependent

The settings available through the MEBx screens, and the default values of those settings are determined by the PC manufacturer.

Accessing MEBx settings is vendor-dependent

The PC hardware vendor (the OEM) determines the management engine BIOS extension (MEBx) parameters you can access and/or change.

Changing MEBx settings during or after setup

You can change MEBx settings manually during setup, if these settings are available (the available settings depend on your PC manufacturer). You can also change MEBx settings post-setup.

Changing settings after setup can be done deskside (manually) or through the configuration service, after a secure communication path has been established to the Intel AMT capabilities on the PC.

Typical information entered through MEBx

Typically, when setting up PCs to enable Intel AMT, you must enter some information into the MEBx manually or via a USB-key storage device. This information includes:

- Server address for the configuration service
- Communication port for communication with the configuration service
- VLAN (virtual LAN) setting
- PID and PPS

Figure 4-4 shows a sample BIOS extension screen.

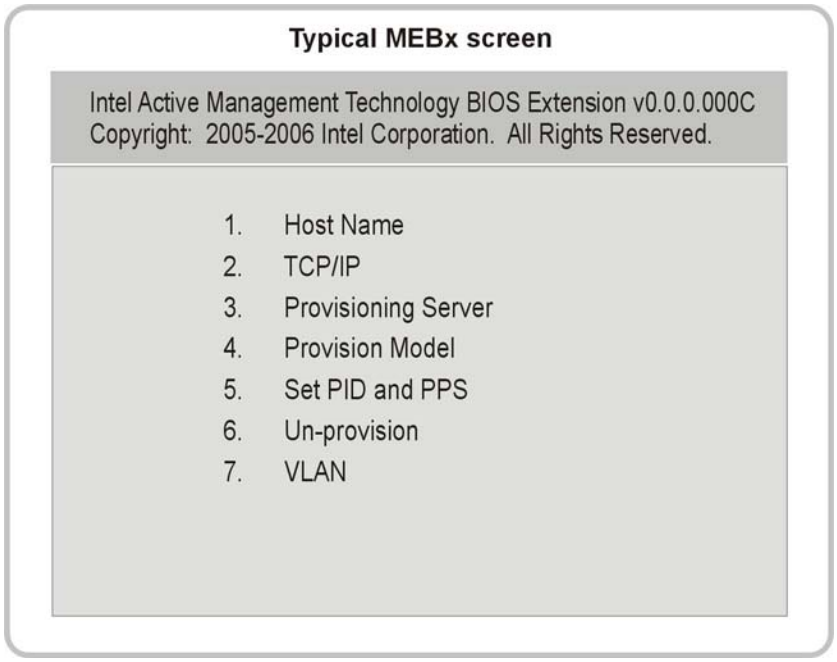

Figure 4-4. Example MEBx screen. The parameters you can access through the MEBx screens are vendor-dependent.

Common MEBx parameters

Table 4-3 lists common setup parameters and some typical or Intel-recommended defaults. The next few pages describe some of these setup parameters in more detail.

Table 4-3. Common MEBx setup parameters

Parameter	Default	Description
Administrator username and password	*admin-admin*	By default the administrator username-password pair is set to the OEM-defined values (refer to your OEM documentation).
Host name	*ProvisionServer*	The host name is the name of the DHCP server or other host device. If you do not enter a host name, Intel AMT will automatically query the network for a device called *ProvisionServer*, and select that device as the host.
TCP/IP	Enabled	The administrator can configure whether Intel AMT gets its IP address from a DHCP server or has a statically defined IP address.
Provisioning server	Defined by DHCP and DNS	By default, Intel AMT performs a DNS lookup to find the address of the configuration (provisioning) server. If DHCP and DNS are not available, you must manually enter the server's IP address and TCP communication port number.
Server address	*0.0.0.0*	The IP address of the configuration server being used to configure Intel AMT. A value of 0.0.0.0 means that Intel AMT will try to obtain the actual IP address of the server by performing a DNS lookup for a host named *ProvisionServer*.
Server port	*9971*	The port address to which Intel AMT will send communications to the configuration service. By default, port 9971 is used to establish a connection to the CS.
Provisioning model	Enterprise	By default, Intel AMT is set to enterprise mode. However, your hardware vendor may set this field to small-business model, as requested for your environment.
PID and PPS	No default value	These values are defined during setup of Intel AMT.
SOL / IDE-R	Enabled	The serial over LAN (SOL) and integrated drive electronics redirection (IDE-R) setting activates the console redirection and remote-boot capabilities of Intel AMT.
VLAN	Enabled	The VLAN setting allows the out-of-band communication to be assigned to a logical, virtual LAN that is separate from the in-band communication from the LAN. When VLAN is enabled, you must enter the VLAN ID, which is typically a value between 0 and 4095.

Changing usernames and passwords

Note the following considerations when changing the factory-default username and password.

- Default username and password. The factory-default username and password are defined by the hardware vendor, and should be provided in the PC's shipping container or manual, on a sticker, or via some other method. In some cases, as specified by the customer, the default username and password may be left unspecified (blank).
- Enter correct administrator username. Do not assume the value of the administrator username (for example, *admin* versus *administrator)*. Make sure you enter the correct username-password pair, or the setup process will fail. The username-password pair for each PC is provided by your OEM.
- Change the username, not just the password. When working with localized BIOS, the authentication process requires that you change only the default password. However, best practices suggest that you also change the administrator username from the factory default to something more unique.
- Help prevent masquerade attacks during configuration. The requirement to change the default password the first time you enter MEBx (during setup) helps prevent masquerade attacks later during Intel AMT configuration, based on a presumably well-known factory default username/password.

Security considerations

Refer to the security section of this guide, and to the appendix on best practices, for reference information on establishing robust username-password pairs.

PID-PPS

The provisioning ID (PID) and provisioning passphrase (PPS) are required to establish secure communication during configuration. The PID is a 64-bit quantity sent in the open. The PPS is a 254-bit quantity that is a secret shared between Intel AMT and the CS. Both are case-insensitive and consist of alphanumeric characters.

An example of a PID-PPS pair could be:

- PID: *D64G-GXY6*
- PPS: *MD97-QC7R-TQJG-3V2W-W7PV-RBDC-VTRC-D797*

If you enter the PID and PPS manually through the MEBx screens, the MEBx firmware checks for checksum characters embedded in the values.

- PID: The last character is expected to be a checksum of the previous seven characters.
- PPS: The fourth character in each group of four characters is expected to be a checksum of the previous three characters.

The checks help reduce the possibility of operator error when entering these values. For hardware vendors and third-party software vendors, the SDK contains source code for a sample function that generates PID/PPS pairs with embedded checksums.

The PID-PPS pair for each PC must be entered in the PSK repository of the configuration server. For example, the repository for a configuration service could be stored in a file called *psk.repository.xml*.

Server address

By default, the IP address of the CS server is set to 0.0.0.0. A value of 0.0.0.0 means that Intel AMT will try to obtain the actual IP address of the CS server by performing a DNS lookup for a host named *ProvisionServer*.

If the DNS is unable to resolve the host name, you must manually enter the IP address of the CS. This should be done during setup, via the BIOS extension screen.

Port

This parameter is the port address to which Intel AMT will send communications to the configuration service. By default, port 9971 is used to establish a connection to the CS. However, if the CS has been configured to listen on a different port, you must manually specify the port on which the CS is listening. This should be done during setup, via the MEBx.

VLAN Setting

The virtual local-area network (VLAN) setting applies to the out-of-band communication traffic sent and received by Intel AMT. The VLAN setting allows communication to be assigned to a logical, virtual local-area network that is separate from the in-band communication on the LAN.

If the PC's operating system is using a VLAN identifier for network communication, then Intel AMT must also use the same VLAN identifier.

The use of a VLAN for out-of-band communication is enabled or disabled through an option in the MEBx. When VLAN is enabled, you can specify a different VLAN from the PC's operating system (the host). You can also disable VLAN to configure the PC's operating system to operate without a VLAN definition.

DNS not available

In some environments, DNS is not available, and the PC cannot automatically obtain the IP address of the configuration server through a DNA lookup. In these environments, you must manually enter the IP address of the CS during the setup procedure. You can also manually enter a static IP address later, during a manual configuration process, by using the BIOS extension screen.

Using the same IP address

If Intel AMT will share IP addresses with the host processor using a DHCP-assigned address, both the host (the PC's OS) and Intel AMT must be configured to use the same VLAN. Also, the DHCP server should be configured to use the same VLAN.

Manual setup
If a flash device will not be used to enter setup parameters, you must perform the setup process manually.

LPR
The LPR is the file containing the information required to establish the initial, bootstrap networking and TLS security credentials: administrator password, provisioning passphrase (PPS), and provisioning ID (PID).

Configuration profile
The configuration profile is a file containing the Intel Management Engine power policies, as well as the Intel AMT Kerberos settings, access control lists, certificates and keys, and the settings that activate Intel AMT.

Use current password
USB-key local provisioning can be performed only if the USB-key local-provisioning file contains the current MEBx password.

Note:
If the BIOS does not find a USB storage device, or if it does not find the USB-key local provisioning file on the device's storage medium, it skips the following steps and proceeds with the normal boot flow.

Using USB-key local provisioning for setup

The most obvious way to specify MEBx settings is by typing the administrator password, PPS, and PID into the BIOS and MEBx configuration screens. However, this can be a tedious and error-prone process. An easier way is to use a USB storage device to enter that information for you, if your BIOS manufacturer allows booting from a USB device.

USB-key local setup is performed by reading a USB-key local provisioning file into Intel AMT via a USB storage device. The USB-key local provisioning file contains unique USB-key local provisioning records (LPRs). Each unique LPR is read into Intel AMT on a single PC.

The process is simple: The USB-key local provisioning file is written to a portable USB storage device by the configuration service. When the USB storage device is plugged into a PC, the BIOS reads a record from the USB-key local provisioning file, and passes it to the MEBx. The MEBx parses the record and passes each of its entries to the appropriate management-engine firmware component.

USB-key local provisioning follows these general steps:

1. The IT technician uses a configuration service (CS) user interface program (such as the CS) to send a request to the CS to generate a list of USB key local provisioning records.
2. The CS generates the list of USB-key LPRs.
3. The CS stores the list of USB-key LPRs in the SC database.
4. The CS returns the list of USB-key LPRs to the user interface program.
5. The technician acquires the USB-key LPR list. The technician does this by inserting a portable USB storage device into a physical USB port on the machine that hosts the user interface program. The user interface program writes the USB-key LPR list. The technician then removes the USB storage device from the USB port.
6. The technician removes the Intel AMT-enabled PC from its box, plugs in the system cables and the USB storage device, and powers the system on.
7. As the system boots, the BIOS looks for a USB storage device.

USB local provisioning

For detailed information about USB-key local provisioning, refer to the USB-key local-provisioning architecture design specification for the Intel Management Engine. Contact your Intel representative for a copy of this specification.

8. As soon as BIOS finds a USB storage device, it looks for the USB-key local provisioning file on the device's storage medium.

Caution

Do not power down or otherwise interrupt the PC during the setup process. Each PC's unique ID is associated with the specific USB key used to provision Intel AMT for that PC. If the setup process is interrupted, you may have to manually reset that PPS and PID. At worst, the interruption might have voided a PPS-PID pair in the PSK repository, and may prevent the PC associated with that PPS-PID pair from authenticating the configuration service (as well as any remote management server) that attempts to communicate with the system.

9. The BIOS validates the USB-key local provisioning file.
10. The BIOS writes a message to the display that indicates that the USB-key local provisioning file is being processed. The message warns the technician not to power off the system until processing is complete.
11. The USB key device loads BIOS and MEBx settings, including enabling the Intel Management Engine, setting power policies for management-engine sleep states, and enabling Intel AMT.
12. The BIOS reads a single record from the USB-key local provisioning file, places the record in a memory, and places a pointer (to the base address) in the parameter block that is passed to MEBx. The BIOS then invokes the MEBx.
13. MEBx processes the record entries that are relevant to the platform. For each entry, MEBx selects an Intel Management Engine interface endpoint, based on the entry's *ModuleIdentifier* value and a message type based on the entry's *VariableTypeIdentifier* value.

Setup status messages

The vendor-specific BIOS should write a message to the display, letting you know when it is safe to power down the PC.

14. When MEBx is done processing the record, the BIOS will continue the boot process and finish loading.
15. The technician powers down the system.

The system is then ready to be delivered to the user's desk, where Intel AMT can complete its own configuration.

CS available in staging area

An experienced IT administrator can set up an isolated staging environment that fully sets up and configures Intel AMT before PCs are delivered to the user desk. This can be useful in environments in which security is a high priority.

No need to power up PC

PCs with Intel AMT are enabled for out-of-band communication. They do not necessarily have to be powered up in order to establish a connection to the configuration server, or to perform the self-initiated and automatic configuration process. Refer to the next discussion for more information about waking the management engine.

Configuration

Once a PC is populated with its initial security credentials, Intel AMT must be configured for operation in your network environment. In most enterprise environments, Intel AMT will automatically initiate this process as soon as it is set up, connected to a power source, and first plugged into the network.

As soon as the MEBx screens are exited during setup, and BIOS finishes loading, Intel AMT begins sending "hello" packets to the CS listening port. Intel AMT does this to try initiating its own automated configuration, including establishing the unique security certificates. If the CS is not available to Intel AMT in the staging area, configuration will occur later, when the PC is at the user desk and the CS is available in that domain.

After the PC is delivered to the user, connected to a power source and the network, Intel AMT begins sending its hello packets again. Once the connection to the configuration service is established, configuration itself can be a fully automated process, completed for you by Intel AMT and the CS.

General steps for automated configuration

Configuration follows these general steps:

1. The user plugs the PC into a power source and connects the network cables.
2. Intel AMT automatically and periodically sends messages to the configuration service to try to download the expected settings. These messages are called "hello" packets. They allow the configuration service to identify the PC that needs to be configured. If power policies have been set appropriately during setup, Intel AMT can send these messages even before the PC is powered up, and before management agents are installed.
3. The configuration service receives the hello packet and sends back the appropriate configuration settings.
4. The configuration service applies the configuration settings to Intel AMT, then remotely reboots the system so that the settings take effect, and cleans up residual files.
5. The configuration service places Intel AMT in its fully configured state.

The PC is then ready for remote management via the Intel AMT capabilities.

The next several pages describe the configuration profile, hello packets, and networking and security considerations for configuration.

Terminology

- ACL – access control list
- 3PDS – the third-party data store in nonvolatile memory

Configuration profile

The information loaded into Intel AMT by the configuration service is called a configuration profile. This profile consists of:

- System power policies for the Intel Management Engine
- Kerberos settings
- Access control lists for management of realms, individual realms such as the remote-control realm and third-party data store (3PDS), and so on
- Certificates and keys for establishing secure, encrypted communication between the configuration server and the PC
- HTTP digest credentials and HTTP negotiate credentials
- Current date and time
- Settings that activate the capabilities of Intel AMT

You can specify many parameters in the configuration profile, including:

- Power policies for the Intel Management Engine.
- Kerberos settings.
- Security settings, including the administrator ACL, user ACLs or realm ACLs (if Kerberos is not used), and certificates and keys.
- Storage settings.
- Storage admin settings, including the enterprise access control list.
- Event-management settings, such as event filters and subscriptions. This helps you specify the events you want the management console to automatically receive.
- Settings for the network outbreak containment capability, such as filters for known threats and policies. Policies include rate-limits, partial isolation of the user OS by cutting off some communication ports, or full isolation of the user OS from the production network.
- Agent presence settings.

For more information about the Intel AMT parameters you can modify, refer to the documentation for your third-party configuration service. For information about Intel AMT capabilities, refer to the Intel AMT overview section of this guide or to the Intel Web site.

Reinitializing hello packets

Refer to the discussion "Reinitializing the hello-packet sequence," earlier in this section, for information about reinitializing the hello-packet sequence in environments in which PCs have been deployed for some time before Intel AMT is configured.

Hello packet

After Intel AMT locates and connects to the configuration service, it sends its hello packet. The first two bytes of the hello packet are usually 0x0001, unless the PC has a localized BIOS. If you are working with a localized BIOS, the first two bytes of the hello packet will be 0x0000, indicating that new administrator credentials must be set in Intel AMT before setup and configuration to complete successfully.

Table 4-4 describes the format of the hello packet.

Table 4-4. Hello packet format

Byte offset	Content
0	Admin credential set
2	Interface version
4	Retry count (0-14)
8	Device UUID
24	PID

Dynamic and static IP environments

Intel AMT initiates its own automated configuration in both dynamic IP and static IP environments. In dynamic IP environments, Intel AMT uses DHCP and DNS to locate the configuration service. In static IP environments, Intel AMT uses the network information manually entered during setup to locate the configuration service.

Periodic retries for automated configuration

Intel AMT will periodically try establishing the connection to the CS at regular intervals until configuration is complete. A completed configuration is defined by two primary conditions:

- Intel AMT has all required parameters loaded.
- The configuration service has sent the **CommitChanges** command.

Intel AMT will attempt to complete its configuration at these intervals:

- 5 retries on 1 minute intervals
- 5 retries on 10 minute intervals.
- 5 retries on 1 hour intervals.

If the PC is reset or power is cycled during this sequence, Intel AMT will start over, attempting to complete its configuration on 1-minute intervals again.

Establishing a TCP/IP connection

When PCs are configured in enterprise mode, Intel AMT automatically tries to obtain its own network settings as soon as Intel AMT is set up and the PC is connected to power and the network. By default, Intel AMT tries to obtain its networking settings from a DHCP server. Intel AMT then automatically tries to locate the CS server, establishes a network connection to the CS, and then waits for the CS to deliver its configuration settings.

In static IP mode

Intel AMT uses the IP address and other network parameters installed during the setup procedure to locate the configuration server.

No TLS yet

TLS certificates are not established until after Intel AMT has located the configuration service, authenticated the service, and been authenticated in turn using the preshared key (PSK) credentials established during setup.

These general steps are followed to establish a secure TCP/IP connection to the configuration service:

1. Intel AMT sends a request (a hello message, or packet) to the DHCP server for an IP address. The DHCP server returns a reply containing the IP address for Intel AMT, the DNS domain name, and the IP address of the DNS server.
2. Intel AMT sends a request to the DNS server for an IP address of the configuration server.
3. The DNS server returns a reply containing the IP address of the configuration server.
4. Using this information, Intel AMT establishes a TCP/IP connection to the configuration server.
5. The configuration server then authenticates Intel AMT using the preshared key infrastructure (PKI) credentials established during setup.

If this process is unsuccessful, Intel AMT will continue to try establishing the connection until configuration is complete.

CS default port

By default, Intel AMT is configured to use port 9971 for CS traffic.

Encrypted communications

All configuration information sent over the TCP/IP connection during this process is encrypted.

PPS is in PSK repository

The provisioning passphrase is stored in the server's preshared-key (PSK) repository of known PID-PPS pairs.

Customizing batch files

You can customize the batch file used to clean up configuration files so that it performs additional tasks. For example, you could modify the file to include an e-mail to the management console or to update a database with information about the PC's deployment or readiness for build.

Establishing TLS and configuring Intel AMT

Once the TCP/IP connection is established and secured via the preshared key credentials, the configuration process continues, following these general steps:

1. Intel AMT sends a hello packet. Intel AMT sends the configuration service a hello packet with the PC's device-specific information: UUID, PID, IP address, ROM version numbers, and firmware version numbers
2. The CS identifies Intel AMT and its configuration profile. The configuration service uses the PID from the hello packet to look up the PPS associated with Intel AMT on that PC.
3. The CS establishes a secure TLS session. The configuration service establishes a secure TLS session with Intel AMT, using the PPS found in the server's PSK (preshared key) repository.
4. The CS logs into the Intel Management Engine using the factory-default HTTP digest network-administrator username and password.
5. The CS loads Intel AMT with the configuration profile. The profile includes power policies, Kerberos settings, certificates and keys, access control lists, and information required to activate the capabilities of Intel AMT.
6. The CS activates the settings. The configuration service sends a **CommitChanges** command to reboot the PC, and activates the configuration settings for Intel AMT. The configuration service then uses a batch file to clean up files created during the configuration process.

When configuration is complete, Intel AMT is in its fully configured state, ready for use in the enterprise environment. You can then use the SOAP interface to change the configuration profile as needed to suit your enterprise environment. The configuration-management section in this guide explains how to unconfigure and reconfigure Intel AMT.

Certificates

A new security certificate must be established if you change the host (the PC's OS) name or move the PC.

Changing a host name or moving the PC

The PC host (operating system) name and its location are part of its security certificate. When Intel AMT is first set up, and the PC is moved to its working location, connected to power, and plugged into the network, the configuration process – including generation of the certificate – will typically be self-initiated and automatic. If an OS name is changed or the PC is moved to a new location, you must reconfigure Intel AMT so that a new certificate can be generated with the new location information.

In dynamic IP environments, this can be performed by unconfiguring Intel AMT, moving the PC to its new location, then reconnecting the system to power and the network. Intel AMT will automatically initiate its configuration process again, send its hello packets, and try to reconfigure itself. Unconfiguring and reconfiguring processes are described in the configuration-management section of this guide.

In static IP environments, you can unconfigure Intel AMT using an automated script or some other third-party management tool. To reconfigure Intel AMT, you must perform the manual part of the setup and configuration processes again. This includes specifying the new OS name, domain name, IP address, or other required information through the MEBx screens. These processes are described in the quick-start section of this guide.

Unconfiguring Intel AMT

Refer to the configuration-management section in this guide for information about unconfiguring and reconfiguring Intel AMT.

Returning to factory defaults

Sometimes you need to erase a configuration profile and return Intel AMT to its unconfigured state for use in a new location or for a different purpose. This process is called unconfiguring Intel AMT.

Unconfiguring Intel AMT erases the configuration profile and other configuration information, but leaves the security credentials established. This allows you to move the PC to a new location or reconfigure the PC remotely for a new use, without having to set up Intel AMT again. This process does not return Intel AMT to its factory-default state.

You might also want to erase both the configuration profile and the security credentials in order to fully disable Intel AMT remote management, such as for PCs that will be moved to less secure environments. This process is called erasing the security credentials.

Erasing both the configuration profile and the security credentials returns Intel AMT to its factory-default state. In this state, you must set up Intel AMT and allow automated configuration again before the capabilities will be available for remote management.

The configuration management section of this guide explains unconfiguration and erasing the security credentials in detail.

For more information

Once Intel AMT has been set up and configured, it can be unconfigured or reconfigured as needed for your business environment. Setup and configuration processes are provided in the quick-start section of this guide.

Background and reference Information about security methods and technologies can be found in the security section of this guide and in the best-practices appendix.

Section 5
Configuration management

Intel® AMT

Intel® Active Management Technology (Intel® AMT) is one aspect of the new hardware-based capabilities of Intel® vPro™ technology

Background information

For detailed information about networking and security in an enterprise environment, refer to the security section and the setup and configuration section of this guide.

Introduction

IT administrators sometimes need to reconfigure Intel AMT because the PC's location or intended use has changed. For example, the administrator may need to:

- Move and assign a PC to a new user or location
- Reconfigure a PC for use in a different environment
- Enable the Intel AMT capabilities in PCs that were previously deployed in the enterprise
- Remove a PC from the management domain

When a PC is being reused within the organization, it is not always necessary to erase and reestablish all security credentials for Intel AMT. Often an IT administrator will perform a "partial unprovisioning." In a partial unprovisioning, the administrator simply unconfigures the Intel AMT settings, moves the PC, and allows Intel AMT to automatically reconfigure itself for its new location or use.

In some cases, an administrator might remove a PC from the management domain. In environments where security is a high-priority concern, it may be advisable or necessary to fully erase all initial security credentials, not just authentication certificates and configuration information. This includes erasing the administrator password, provisioning passphrase (PPS), and provisioning ID (PID), and returning Intel AMT to its factory-default state.

This section explains the general steps for unconfiguring Intel AMT, erasing setup information, reestablishing bootstrap security credentials (setup), and reconfiguring Intel AMT. This section covers these general topics:

- Overview of configuration management
- Unconfigure Intel AMT
- Modify configurations
- Setup and reconfigure Intel AMT

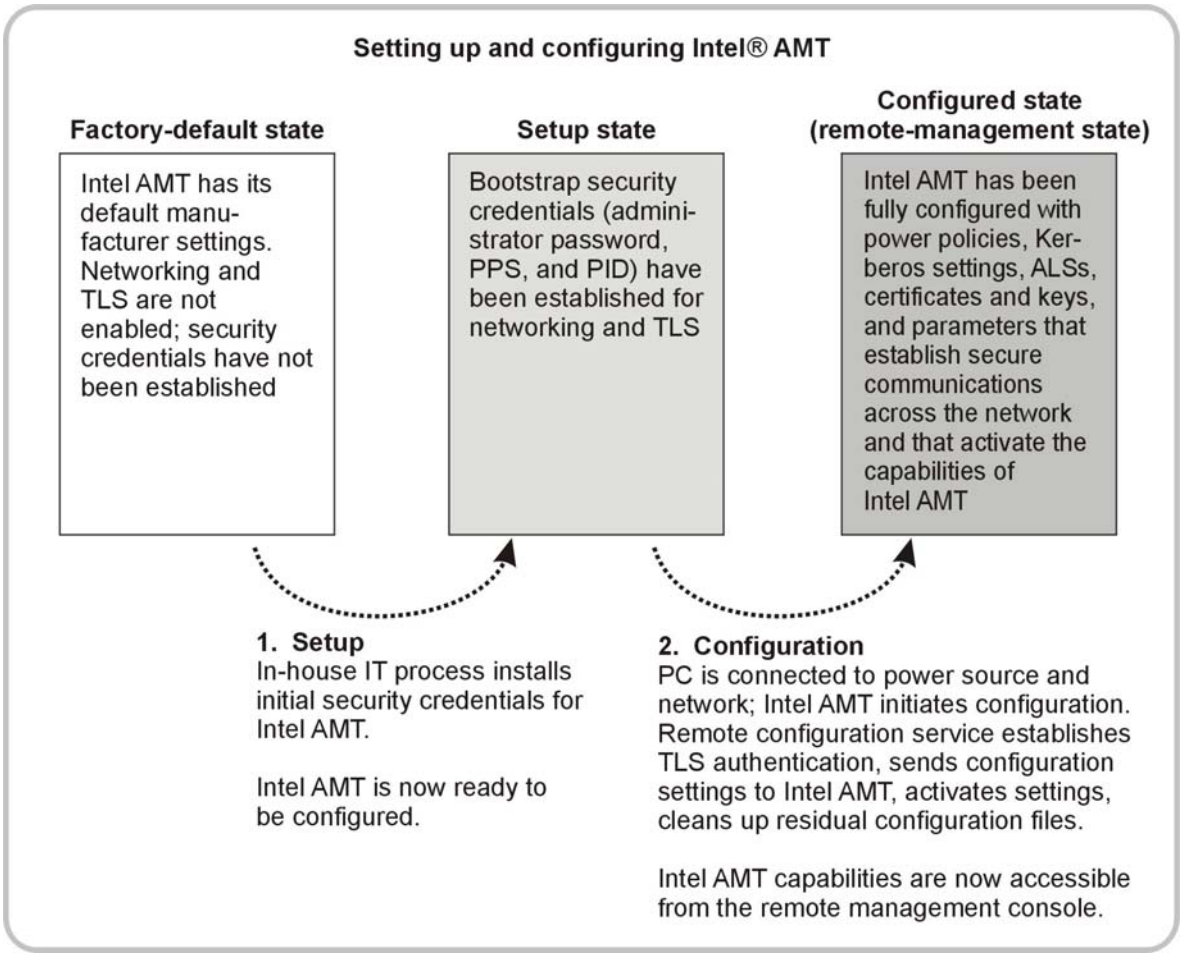

Figure 5-1. Setting up and configuring Intel AMT. Intel AMT is set up and configured so that the powerful remote-management capabilities are available to authorized IT technicians.

Figure 5-1 (above) briefly describes the processes for setting up and configuring Intel AMT. Figure 5-2 briefly describes the processes for unconfiguring Intel AMT and erasing the setup information (the initial security credentials for Intel AMT).

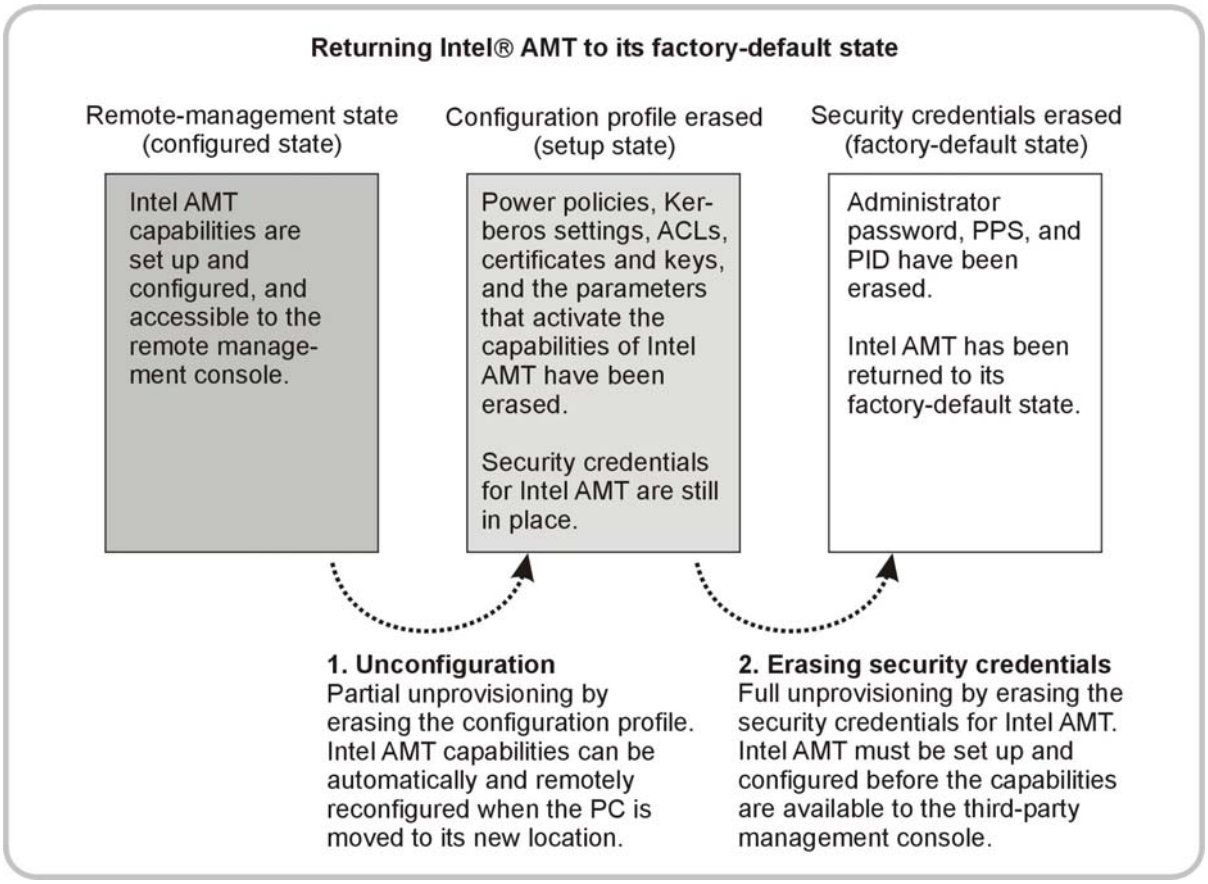

Figure 5-2. Unconfiguring Intel AMT and erasing security credentials. Unconfiguring Intel AMT returns the technology to its setup state. Erasing security credentials returns Intel AMT to its factory-default state.

Overview of configuration management

Setup and configuration of Intel AMT is established by setting up initial security credentials (the setup process), and by loading Intel AMT and the Intel® Management Engine with the configuration profile (the configuration process).

- Configuration profile – a set of configuration data that is applied to the Intel Management Engine and the Intel AMT settings of one or more PCs by the configuration service.
- Security credentials – a set of information that allows Intel AMT to establish its initial security credentials: administrator password, PPS, and PID.

Unconfiguring Intel AMT erases the configuration profile and returns the system to its unconfigured – but still setup – state. This is typically done to disable the PC for remote management, change fundamental configuration settings of Intel AMT (or the PC), move the PC to a new location, or configure the device for a different use within the enterprise.

Erasing the initial security credentials for Intel AMT returns Intel AMT to its factory default settings. This is typically done when an enterprise wants to make sure previously setup security authorizations have been fully erased for that machine.

Terminology

- MEBx - Intel Management Engine BIOS extension
- PID - provisioning ID
- PPS - provisioning passphrase

Intel AMT status

Because the BIOS, MEBx, configuration service, and management software are vendor-dependent, different terms may be used to indicate the status of Intel AMT. Figure 5-1, earlier in this section, shows the states of Intel AMT. Tables 5-1 and 5-2 list some terms that could be used to indicate those states.

Table 5-1. Setup and configuration states

State	Description	Some possible terms for status
Factory-default state	Intel AMT has its factory-default settings, as defined by the PC manufacturer. Intel AMT has not been set up with security credentials or configured.	Factory-default Unprovisioned Preprovisioned ProvisioningStatePre
Setup state	Intel AMT has been set up. The administrator password, PID, and PPS (the initial, bootstrap security credentials) have been established.	Setup Setup mode In-Setup In Provisioning ProvisioningStateIn
Configured state	Intel AMT has been configured. The security settings, network parameters, Kerberos settings, access-control lists, and other information required to activate Intel AMT have been configured. Intel AMT can now be remotely managed through a third-party application.	Configured Operational Provisioned Post-provisioned ProvisioningStatePost

Table 5-2. States for unconfiguring and erasing setup information

Action	State	Description	Some possible terms for status
Operational state	Configured state	Intel AMT is configured and operational.	Configured Operational Provisioned
Unconfigure (partial unprovisioning)	Setup state	Intel AMT has been unconfigured. The Intel AMT configuration profile has been erased. However, the setup information (administrator password, PID, and PPS) remain in the system.	Unconfigured Partially unprovisioned
Unconfigure and erase setup information (full or waterfall unprovisioning)	Factory-default state	Intel AMT has been returned to its factory-default settings, as defined by the OEM. All Intel AMT setup and configuration information (including administrator password, PID, and PPS) have been erased. You must perform the setup and configuration processes again before you can remotely manage the PC through Intel AMT capabilities.	Unprovisioned Fully unprovisioned Waterfall unprovisioned Factory defaults OEM defaults

Quick-start procedures
Refer to the quick-start section of this guide for procedures to set up and configure Intel AMT for both dynamic IP and static IP network environments.

Static IP environments
In static IP environments, you can unconfigure Intel AMT using an automated script or other third-party management tool. To reconfigure Intel AMT in a static IP network, you must perform the manual part of the setup and configuration processes again.

Changing setup type
The operational mode (enterprise or small business) can be changed only when Intel AMT has been returned to its factory default settings. Restoring Intel AMT to factory mode is done through the MEBx or over the network using the SOAP interface.

Changing a host name or moving the PC

When Intel AMT is first set up, the PC is moved to its working location, and the system is connected to power and the network, the Intel AMT configuration process will typically be self-initiated and automatic. As soon as the PC is connected to a power source and plugged into the network, Intel AMT will initiate and complete its configuration for you, including generating security certificates.

The security certificates for Intel AMT include information such as the PC's host (operating system) name and its location. If an OS name is changed or the PC is moved to a new location, you must reconfigure Intel AMT so that a new certificate can be generated with the new location information.

Different network environments

The process for reconfiguring Intel AMT will depend on your networking environment:

- Dynamic IP networking: Intel AMT is typically unconfigured, the PC is moved to its new location, the PC is reconnected to power and the network, and Intel AMT is allowed to automatically reconfigure itself.
- Static IP networking: Intel AMT is unconfigured, its static IP information is erased, and the manual setup process is followed again to set up initial security credentials for the Intel AMT capabilities at the new location. This includes specifying the new OS name, domain name, IP address, or other required information through the MEBx screens. Intel AMT can then perform its own automatic configuration at the PC's new location.

When Intel AMT is unconfigured (but still setup), it stills has security credentials, and can be remotely reconfigured by the configuration service.

Unprovisioning
Restoring Intel AMT to its factory-default state is also called "unprovisioning."

Security credentials
The initial security credentials for Intel AMT consist of the information required to establish the bootstrap networking and TLS security credentials: administrator password, provisioning passphrase (PPS), and provisioning ID (PID).

Configuration profile
A file containing the Intel Management Engine power policies, as well as the Kerberos settings, access control lists, certificates and keys, and settings that activate Intel AMT.

Waterfall unprovisioning
Full unprovisioning is also sometimes called "waterfall" unprovisioning.

Changing setup type
The setup type (enterprise or small business) can be changed only when Intel AMT is in factory mode (the factory-default state). Refer to the unprovisioning procedure, later in this section, for information on returning Intel AMT to its factory-default state.

Erasing security credentials and network settings

You can use a third-party application or the MEBx to return Intel AMT to its factory default state. This process typically erases both the configuration profile and the initial security credentials for Intel AMT, including erasing the administrator password, PID, and PPS. Erasing security credentials and networking information can be useful when PCs will be disposed of to less secure environments or to outside organizations.

Once Intel AMT is returned to the factory-default state, you can no longer access the Intel AMT capabilities from the remote management console. To put Intel AMT back in operational mode, where it can be remotely managed through a third-party console, you must perform the Intel AMT setup and configuration processes again. In more secure environments, establishing the initial security credentials for Intel AMT is typically done via a deskside visit.

Unconfiguring the technology

There are two levels of removing configuration and setup information for Intel AMT. The first level is unconfiguring, and the second level is "unsetup" – basically, erasing security credentials. These levels are also called partial unprovisioning and full unprovisioning.

Partial unprovisioning allows Intel AMT to retain the administrator password, the last installed provisioning passphrase (PPS), and the provisioning identifier (PID). When Intel AMT has been unconfigured (partially unprovisioned), it can be reprovisioned from a remote console, without a deskside visit.

Note:

In environments in which security is a high-priority concern, Intel recommends that you change the administrator password, PPS, and PID before returning the system to its default configuration.

Full unprovisioning erases all setup and configuration information, including the administrator password, PPS, and PID. When Intel AMT has been returned to its factory-default state (all security credentials have been erased), it cannot be set up again remotely. Instead, the setup procedure, which typically requires a deskside visit, must be followed in order to reestablish security and networking credentials. After that, Intel AMT can initiate and complete its own remote, automated configuration as usual.

This section describes the unprovisioning and reprovisioning processes.

Check configuration status

To check the status of Intel AMT on a particular PC, follow these general steps:

1. Using your third-party software, display a list of all PCs with Intel AMT on the network.
2. Use your system's search function to locate the specific PC by its UUID or device name.
3. If necessary, select the option that displays the PC's attributes.

Your third-party software should then display the attributes for that device, including the provisioning status, similar to the states listed in Table 5-3.

Table 5-3. Possible status types for Intel AMT[1]

Status	Definition
Provisioned	Indicates that Intel AMT is set up and configured successfully.
Provisioning	Indicates that Intel AMT is still in the configuration process.
Unprovisioned	Indicates that Intel AMT is not yet configured.
Failed	Indicates that the setup and configuration process for Intel AMT has failed. In this case, you should check your configuration service (or management console) event log to find out what happened during the configuration process to cause the configuration or unconfiguration to fail.

[1] Refer to tables 5-1 and 5-2, earlier in this section, for other possible terms that could be used to indicate the status of Intel AMT.

Erase only configuration information using an API

There are some application programming interfaces (APIs) in the market which allow you to unconfigure Intel AMT (partial unprovisioning), rather than erase all setup and configuration information as a single process (full unprovisioning). This is useful when you want to reconfigure the system for use in a different location or for a different use.

Status terms

Refer to Tables 5-1 and 5-2, earlier in this section, for a list of possible status terms.

Follow these general steps to unconfigure Intel AMT, erasing only the configuration profile:

Note:

In environments in which security is a high-priority concern, Intel recommends that you change the Intel AMT administrator password, PPS, and PID before performing the partial unprovisioning (unconfiguration).

1. Using your third-party management software, change the administrator password for Intel AMT.
2. Using your management software, change the PPS and PID to values appropriate for Intel AMT at the PC's new location (or use).
3. Now display the list of all PCs with Intel AMT on the network.
4. Use your system's search function to locate the specific PC by its UUID or device name. The system should display the device status, and may also list convenient operations you can perform. You can unconfigure Intel AMT if the device status indicates that Intel AMT is configured or configuring; failed; or a similar term.
5. Select the option to partially unprovision (unconfigure) Intel AMT. The system should then display a prompt asking you to confirm the partial unprovisioning process.
6. Confirm that you want to perform the partial unprovisioning. The system will then erase the configuration profile for Intel AMT for that PC.

Status messages

Some BIOS implementations will ask you to wait until the unconfiguration process is complete before performing other tasks. Other implementations will simply wait until unconfiguration is complete before allowing you to perform other tasks.

It typically takes a few seconds or less to partially unprovision Intel AMT. If the operation was successful, the status of Intel AMT for that PC should be changed to indicate that Intel AMT is now unconfigured, setup, in-setup, or a similar term. When the process is complete, the system may display a message saying "Process complete" or "Process failed," or a similar message. The PC is now ready to be moved to its new location or reconfigured for its new use.

Note that bootstrap security credentials, which allow remote communication with Intel AMT, are still established after this process. In its setup state, Intel AMT can still be accessed by the configuration service. This means Intel AMT can reconfigure itself automatically when reconnected to a power source and plugged back into the network.

Erase both setup and configuration information using third-party software

You can erase setup information and return Intel AMT to its factory-default settings over the network using a third-party application and the SOAP interface. Follow these general steps to unconfigure Intel AMT, erase the Intel AMT security credentials, and return Intel AMT to its factory-default state:

1. Display the list of all PCs with Intel AMT on the network.
2. Use your system's search function to locate the specific PC by its UUID or device name. The system should display the device status, and may also list convenient operations you can perform. You can unconfigure Intel AMT and erase security credentials if the device status indicates that Intel AMT is setup or in-setup; configured or configuring; failed; or a similar term.
3. Select the option to unprovision Intel AMT. The system should then display a prompt asking you to confirm the unprovisioning process.
4. Confirm that you want to perform the unprovisioning. The system will then erase the configuration profile and security credentials for Intel AMT.

It typically takes a few seconds or less to fully unprovision Intel AMT. If the operation was successful, the status of Intel AMT for that PC should be changed to indicate that Intel AMT is now unprovisioned.

When the process is complete, the system may display a message saying "Process complete" or "Process failed," or a similar message. Once Intel AMT is returned to its factory-default state, it is no longer available to management applications from the management console. To put Intel AMT back in operational mode, you must perform the setup and configuration processes, as described in the quick-start section of this guide.

Status terms

Refer to Tables 5-1 and 5-2, earlier in this section, for a list of possible status terms.

Status messages

Some BIOS implementations will ask you to wait until the unconfiguration process is complete before performing other tasks. Other implementations will simply wait until unconfiguration is complete before allowing you to perform other tasks.

BIOS and MEBx
Access to the BIOS and MEBx screens is vendor-dependent.

"Waterfall Unprovisioning"
Unconfiguring Intel AMT and erasing setup information is sometimes called full "waterfall" unprovisioning.

Erase both setup and configuration information using the BIOS extension screen

You can also erase the Intel AMT setup and configuration information through the MEBx screens. Follow these general steps to unconfigure Intel AMT and erase security credentials through the MEBx.

1. Use your third-party management software to enter the MEBx screen. You should be prompted to display the next configuration screen.
2. Press the appropriate key to enter the MEBx configuration screen (refer to Figure 5-3 for a sample MEBx screen).
3. In the MEBx screen, select the option to unprovision (or unconfigure) Intel AMT.
4. If prompted, confirm that you want to erase all setup information and return the Intel AMT for this PC to the factory-default settings.

Intel AMT is then unconfigured, its security credentials (including administrator password, PID, and PPS) are erased, and Intel AMT is returned to its factory-default state.

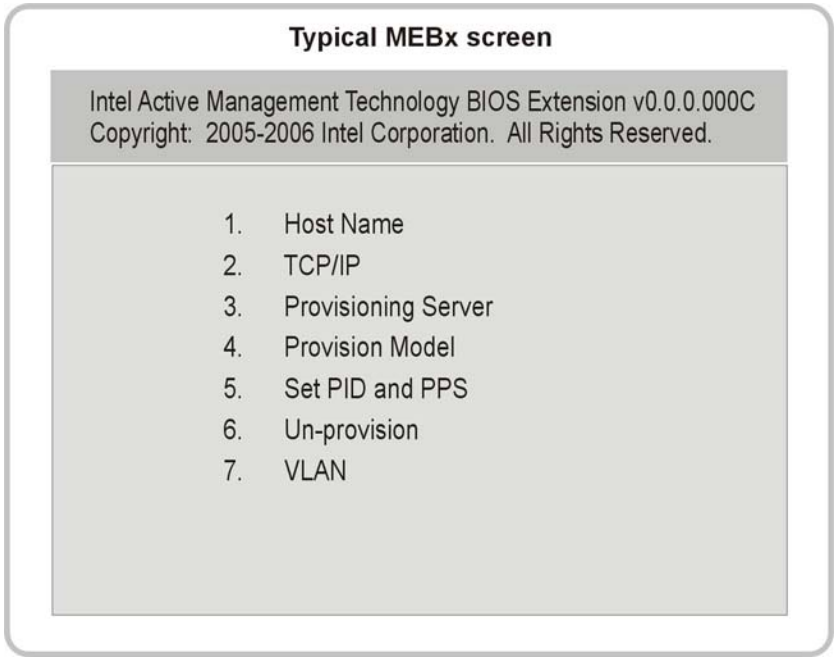

Figure 5-3. Sample MEBx configuration screen. The MEBx screen gives authorized IT administrators access to MEBx settings and the provisioning status of Intel AMT.

Changes made to settings during unconfiguration

When Intel AMT is returned to its factory-default state, the following changes are made to memory, configuration settings, access-control lists, and so on:

1. Certificates are erased from the nonvolatile memory.
2. The nonvolatile storage area is cleared.
3. The event log is cleared, and all transient filters are removed from the nonvolatile memory.
4. All access control lists (ACLs) assigned by the security administration interface are cleared, and the administrator username and password are reset to default values (admin/admin).
5. The storage factory-partner ACL (FPACL) entries are left intact. If the default FPACL entries have been modified, those modifications are retained.
6. The storage enterprise ACL (EACL) list is deleted, and the ACL is restored to its factory-default state (cleared).
7. If the global storage parameters were modified, they will be restored to their default values. This applies to the default values of *MaxPartnerStorage* and *MaxNonPartnerTotalAllocationSize*.
8. Hardware asset information is erased from nonvolatile memory.
9. The hardware is reset.

Once Intel AMT is returned to its default settings, Intel AMT is no longer available to management applications from the remote management console. To restore Intel AMT to operational mode, you must perform the setup and configuration processes again.

Factory-partner ACL

The storage factory-partner ACL (FPACL) entries are left intact when setup and configuration information is erased. Only modifications made to the default FPACL entries are retained.

FPACL list modifications are retained

In some environments, the FPACL list has been modified from its default state. For example, entries have been added, removed, or modified. If the FPACL list has been modified, those modifications remain in the system. The FPACL list is not changed when other settings are returned to the factory defaults.

However, your PC vendor might provide a means of restoring the default FPACL list to its default state. This capability is usually provided through a command option that you would perform *before* restoring Intel AMT to its factory-default state. Refer to your PC vendor's system information to see if such an option is provided.

Administrator password

At the customer's request, the PC vendor may ship Intel AMT with a blank administrator password. The first time you enter an administrator password, that password becomes the factory-default value.

If security credentials are subsequently erased and Intel AMT returned to its factory-default state, the administrator password is not reset to a blank field, but to the first defined password.

Conditions that may prevent unprovisioning

There are a few conditions that may prevent you from being able to unconfigure Intel AMT and erase security credentials. For example, if another IT technician is accessing the MEBx screens (MEBx is active) for that PC, you would not be able to unconfigure Intel AMT or return Intel AMT to its factory-default settings until the other technician exited MEBx.

Note

It is possible that a power interruption (such as unplugging the PC from its power source) could prevent Intel AMT from being returned to its factory-default state. However, Intel AMT includes mechanisms to help mitigate these circumstances during an unprovisioning process.

If the unprovisioning operation fails, the status for Intel AMT will be unchanged. If this happens, check your configuration-service event log (or the event log for your management console) to note error messages or significant events logged during the attempt to return Intel AMT to its default state.

Modify configurations

IT administrators sometimes want to reconfigure a PC for a different use. The next several procedures explain the general steps to check and modify the Intel AMT configuration for a PC, and change the administrator password.

You can modify the configuration profile for Intel AMT if your third-party management software supports this feature.

Changing the profile

You can change many settings in the configuration profile. For example, you can enable or disable SOL/IDE-R, alerting, system defense features, and so on.

Check and modify Intel AMT configuration

Follow these general steps to manually check and/or modify the Intel AMT configuration information for a PC:

1. In your third-party software, select the device-management feature.
2. Display a list of all PCs with Intel AMT on the network.
3. Use your system's search function to locate the specific PC by its UUID or device name. If the status of the device is unconfigured, you can continue with this procedure.
4. Select a PC and display its detailed configuration information.
5. To modify the Intel AMT configuration, select the appropriate edit, disable, or enable option for each of the appropriate configuration parameters.
6. When you have finished modifying the configuration, submit your changes.

The management software should then update the listing with the new configuration information.

Change the administrator password for a device

There are two ways to change the security credentials for Intel AMT: through the MEBx screens or through a USB key storage device. Some third-party management applications support a Web interface for – subject to authentication and authorization – changing information in the MEBx screens. Check with your third-party software vendor to find out if the management application or console offers features for changing security credentials for Intel AMT.

Changing the password via device-management features

Follow these general steps to manually change the administrator password for Intel AMT:

1. In your third-party software, select the device-management feature.
2. Display a list of all PCs with Intel AMT on the network.
3. Use your system's search function to locate the specific PC by its UUID or device name.
4. Select a PC and display the detailed Intel AMT configuration information for that device.
5. Select the edit option for the administrator password for Intel AMT on this PC. The system should display the password-change fields.
6. Enter the new password.
7. Make sure the new password is correct.
8. Submit your change, confirming the change if requested.

The system should then update the password in the configuration information for the Intel AMT capabilities of this PC.

Changing the password through the password listing

Typically, you can also change the administrator password for Intel AMT through the general listing of passwords for devices on your network. Follow these general steps to change the administrator password through the list of all system UUIDs and passwords.

1. In your third-party software, select the device-management feature.
2. Select the management feature for administrator passwords. The software should provide you with a list of all UUIDs and associated passwords.
3. Use your system's search function to locate the specific PC by its UUID or device name.
4. Select the edit feature for the UUID of the PC for which you want to modify the password. The system should display a password-change field.
5. Enter the new password.
6. Make sure the new password is correct.
7. Submit your change, confirming the change if requested.

The system should then update the password in the configuration information for the Intel AMT capabilities of this PC, and update the listing of administrator passwords.

Changing manageability mode

Changing manageability mode (for example, to ASF) will automatically return Intel AMT to its factory-default state.

Change manageability mode

Changing the manageability mode is typically done through MEBx during setup of Intel AMT.

Caution:

Changing the manageability mode will fully unprovision Intel AMT – erasing the configuration profile and the initial security credentials for Intel AMT – and return Intel AMT to its factory-default state. To gain remote access to the Intel AMT capabilities again, you must follow the setup and configuration processes. Setup is typically a manual process.

Refer to the setup and configuration section for information about manageability modes.

Set up and reconfigure the technology

Each PC with Intel AMT must be configured with unique security credentials, consisting of PPS, PID, and administrator password. Records of this information are typically available in a database, through your third-party management console, since that information may be needed for a software or hardware repair.

There are two ways to set up security credentials: through the MEBx screens or through a USB key storage device. Some third-party management applications support a Web interface for – subject to authentication and authorization – changing information in the MEBx screens. Check with your third-party software vendor to find out if the management application or console offers features for changing security credentials for Intel AMT.

Setting up Intel AMT

To set up Intel AMT, follow the setup procedures in the quick-start section of this guide.

Set up Intel AMT using the MEBx screens

This general procedure explains how to set up Intel AMT using an existing set of security credentials. Follow these steps:

1. Choose a unique set of security credentials from the list of available credentials in the database.
2. Power up the PC.
3. Using the appropriate keyboard function key (as defined by the PC manufacturer), display the MEBx configuration screen.
4. Log into the MEBx using the current MEBx password.
5. When prompted, change the old MEBx password to the new MEBx password.
6. Select Intel AMT Configuration. The system will prompt you to enter the administrator password.
7. Log in to Intel AMT using the current administrator username and password.
8. Change both the administrator username and password, as described by the best practices listed in the security section of this guide.

Once the administrator password is changed, you can change other parameters, such as TCP/IP information, PID and PPS, VLAN settings, and so on.

MEBx passwords

Anytime you log into MEBx, you must enter the current MEBx password. If Intel AMT has been unconfigured or returned to its factory-default state, you will be prompted to change this password to a new password.

Reconfigure Intel AMT

Reconfiguring is useful when you want to change fundamental configuration settings or configure Intel AMT for a different use. You can remotely reconfigure Intel AMT if the capabilities have already been set up, or if the Intel AMT settings been only unconfigured (the bootstrap security credentials have not been erased).

There is only one step to configuring Intel AMT after the settings have been unconfigured:

1. At the user's desk, connect the PC to a power source and plug it into the network.

If the configuration service is available, Intel AMT will then initiate its own automatic configuration in this new location, including establishing new security certificates. As soon as configuration is completed, the Intel AMT capabilities in this PC are available to the remote management console.

For more information

Information about the initial setup and configuration processes, as well as detailed background information on enterprise security and network configuring is described in the quick-start, security, and setup and configuration sections of this guide.

Refer to the overview and use-case appendices for additional information about using Intel AMT in a managed environment, including overviews of capabilities, general descriptions of proof-of-concept evaluations, and other background information.

Appendix A
Best Practices

Intel® AMT

Intel® Active Management Technology (Intel® AMT) is one aspect of the new hardware-based capabilities of Intel® vPro™ technology

Terminology

- IDE-R – integrated device electronics redirect
- NOC – network outbreak containment
- PSK – preshared key
- SOL – serial over LAN
- TLS – transport layer security

Introduction

This appendix describes recommended best practices for configuring PCs with Intel AMT, and for post-configuration practices.

Best Practices

To realize the full potential of Intel AMT while maintaining the best possible security, Intel recommends several best practices for setting up and configuring Intel AMT.

Recommended practices for setup and configuration

This discussion briefly explains recommended practices for security and networking during setup and configuration of the configuration service and Intel AMT.

Set up Intel AMT using the secure-configuration mechanism

PCs with Intel AMT include support for secure configuration using preshared key-based TLS (TLS-PSK) protocol.

The default mode for configuring Intel AMT requires the use of the TLS-PSK mechanism. This is because some advanced Intel AMT security features require TLS-PSK configuration in order to deliver powerful capabilities in a secure manner. The advanced features include console redirection (SOL), remote boot (IDE-R), agent-presence checking, hardware timers, and isolation circuitry (network outbreak containment, or NOC).

Intel strongly recommends that users and enterprises who deploy PCs with Intel AMT use the TLS-PSK mechanism for secure configuration. This will help prevent unscrupulous users from watching network traffic between the management console and Intel AMT and gaining access to security-related parameters when those parameters are being uploaded to Intel AMT. Such a user could use security parameters to gain access to Intel AMT features and abuse them, for example, by powering off the system or

installing/uninstalling software on that system. Parameters that should be protected include RSA private keys, PRNG secret key, and so on.

Legacy-mode configuration should be done on an isolated wired network

PCs with Intel AMT can be configured in legacy mode. In this mode, the device is assumed to have been configured over an insecure connection. In legacy mode, the device performs with basic Intel AMT capabilities, and does not allow the use of more advanced security capabilities.

Basic capabilities include: "always-available" communication, remote power-up, remote boot, console redirection, persistent event logs, "always-available" alerting, and access to hardware asset information and preboot BIOS settings. The advanced capabilities that are not enabled include agent-presence checking, hardware timers, and isolation circuitry (network outbreak containment, or NOC).

If for some reason Intel AMT is set up and configured in legacy mode for an enterprise, Intel strongly recommends that the configuration be done on a network that is physically isolated from the enterprise operations network. The isolated subnetwork should only contain trusted users. This will help prevent unscrupulous users from watching network traffic and gain access to security-related parameters that can be used to abuse the system.

Username-password pairs should be unique on each Intel AMT system

Intel AMT uses the username-password pair to authenticate IT administrators for managing PCs with Intel AMT. It is recommended that IT administrators use unique passwords when configurating each PC. Otherwise, a malicious person with knowledge of one username-password pair for one PC could not only compromise that system, but any other system with the same username and password.

In an enterprise, where IT administrators have to provision and manage hundreds or thousands of systems, a password management system/process becomes a necessity, as described next.

Configuration server should be able to leverage a secure password management infrastructure

Third-party software vendors who are developing applications for configuration servers are strongly encouraged to integrate a secure password-management infrastructure into the configuration service. This will make password management easier and more secure for IT users.

Examples of a secure password-management infrastructure could be leveraging the Microsoft Active Directory* infrastructure, or any other X.500/LADP directory infrastructure having adequate security to protect the set of username-password pairs. Even the use of a relational database may serve the purpose, as long as adequate security can be built around it to protect the username-password pairs.

These password management mechanisms should securely store the username-password pairs for each PC with Intel AMT, yet provide them to the IT administrator when they need to manage systems. If the management console has an integrated password-management capability, the management console can authenticate itself to Intel AMT. Authentication is performed by automatically selecting the correct username-password pair and supplying it to Intel AMT, via HTTP digest authentication.

Kerberos

If you choose to use Kerberos security, you will need an environment that supports Active Directory.

* Other names and brands may be claimed as the property of others.

Leverage Microsoft Windows* domain-authentication infrastructure by integrating Intel AMT with Microsoft Active Directory*-based Kerberos standard

Intel AMT includes the ability to authenticate IT administrators using Active Directory-based Kerberos protocol. This authentication mechanism delivers seamless integration and CSl ability by making use of existing Microsoft Windows* infrastructures in the enterprise.

This authentication mechanism greatly simplifies adding and removing Intel AMT management privileges for IT users and administrators. The mechanism also eliminates the need for a separate password-management infrastructure.

High-entropy passwords

High-entropy passwords are passwords that are difficult to guess; such as w7_uH9xb. These are words that are not common names or actual words in the language, and hence cannot be found in a dictionary.

Use of strong passwords

Password-management infrastructures should be able to generate high-entropy passwords. Even in the absence of a password-management system, it is strongly recommended that the configuration server have this capability, so that high quality passwords are generated. Leaving the generation of passwords to humans is prone to result in weak passwords (such as common names of people, places, words, etc.) that are subject to dictionary attacks.

Intel AMT requires that passwords meet the following minimum criteria:

Intel AMT requires that passwords used for authentication to the PC meet the following minimum criteria. Passwords must:

1. Be at least 8 characters long.
2. Include only valid characters. Allowed characters are 7-bit ASCII characters in the values of 32-126 inclusive.
3. Not include invalid characters. The following characters are **not** allowed:
   - " (left double quote)
   - . (period)
   - , (comma)
   - : (colon)
4. Have at least one digit character (0, 1, 2, …, 9).
5. Have at least one 7-bit ASCII non-alphanumeric character (such as ! or $).
6. Contain both lowercase (a, b, c, ...z) and uppercase (A, B, C, ... Z) Latin characters, or non ASCII characters (UTF+00800 and above).

The minimum password requirements do not prevent an administrator from using passwords such as *George_1*, *George_2*, *George_3*, etc., each of which is relatively weak and prone to discovery. When such sequential passwords are defined, the pattern can be easily discovered once a few passwords are obtained.

Random strings such as *HoS8V@y$* and *u$8s#R9a* are examples of stronger passwords.

Change the default admin account name

IT administrators should change the default account name for the Admin account. IT administrators should not use commonly occurring account names for administrators, such as *Admin* or *Administrator*. Using a less common account name helps prevent a malicious attack from easily guessing or gaining the account name.

Although security for user systems is established primarily through the administrator's secret password (which prevents others from impersonating the administrator), IT administrators should also choose nonobvious admin account names for better security.

Server-side TLS

In server-side TLS, the Intel Management Engine (on the PC) acts as the server, and the management console acts as the client.

Server-side TLS should be turned on for all communication with Intel AMT-enabled PCs in the enterprise

Intel AMT provides two modes of TLS operation: TLS enabled and TLS disabled. Intel strongly recommends that TLS be enabled at all times to protect the communication of sensitive data between Intel AMT and the management console.

TLS provides channel authentication and encryption to prevent "man-in-the-middle" attacks. In these attacks, an attacker monitors the network activity between a remote console and a PC, and takes over the connection once the connection is established. The attacker then takes control of the device and continues the attack by sending malicious commands.

TLS mutual authentication should be turned on in addition to server-side TLS

PCs with Intel AMT include support for TLS mutual authentication. Intel recommends that enterprises in which security is a high-priority concern use TLS mutual authentication, in addition to TLS server-side authentication. Using TLS mutual authentication helps make sure that a PC's Intel AMT capabilities can be accessed only from a known, designated management station. Once access to Intel AMT capabilities is restricted to a finite set of stations, more restricted controls can be put in place on those stations to provide an enhanced level of security.

Stricter controls could include:

- Limiting physical access to the station, with only authorized personnel having access permission, using electronic badges, card readers, biometric security, or other methods.
- Audit logging, through special software, to log all activities for that station. Audit logging can be used to track malicious activities by both authorized and unauthorized personnel, in order to hold that person accountable for his or her actions.
- Maintaining availability of the latest antivirus patches, antispyware tools, and other anti-malware tools on the station.

Using mutual authentication in combination with stricter access controls to the station reduces the possibility of an IT administrator or others with malicious intent who know the admin username-password pair accessing Intel AMT capabilities from anywhere on the network.

Ensure correct settings in MEBx

MEBx settings are vendor-dependent

The settings available through the MEBx screens, and the default values of those settings are determined by the PC manufacturer.

The MEBx (Intel® Management Engine BIOS extension) screens allow an IT administrator to specify the settings for controlling the PC's security and privacy level from an Intel AMT standpoint. Typical settings that can be enabled or disabled include:

- Local firmware update operation
- Remote firmware update operation
- SOL/IDE-R
- Wake on LAN
- Intel Management Engine

When settings are available through MEBx, the default values for the settings can be specified during the setup and configuration processes. An enterprise should set appropriate values for these settings based on its own security and privacy policies.

Terminology

- DN – a subsystem identifier
- FQDN – fully qualified domain name
- PRNG – pseudo-random number generator
- UUID – universal unique identifier
- PKI – preshared key infrastructure
- PRNG – pseudo-random number generator

Secure methods

Secure methods for obtaining digital certificates include those described in RFC 2511 – Internet X.509 Certificate Request Message Format.

Private keys must not be passed directly to the CA server

The configuration server should never pass the RSA private key directly to the TLS certificate-authority server. The configuration server should pass only a proof of possession of the private key to the TLS certificate-authority server.

PRNG secret keys should be unique

The hardware in PCs with Intel AMT contains a pseudo-random number generator (PRNG). The PRNG is used to generate runtime keys for secure communication. The PRNG algorithm utilizes a secret key to initialize itself and enable itself to generate a series of random numbers.

One of the properties of this algorithm is that the series of (pseudo) random numbers generated by this algorithm will always be the same, as long as it is initialized with the same secret key. Intel strongly recommends that the configuration server generates a unique PRNG secret key for each PC with Intel AMT.

Failure to set up and configure Intel AMT according to the above recommendation will cause all PCs with Intel AMT to generate the same series of random numbers. This means all PCs would generate the same series of keys for secure communication. If someone knows this series (and hence the resulting keys) for one PC with Intel AMT, they would also know the keys for all other Intel AMT-enabled PCs communicating over the network.

Enable secure communication between the configuration server and the TLS certificate-authority server

The configuration server communicates with the TLS certificate-authority server to obtain digital certificates for the RSA public keys that it generates. It is strongly recommended that the configuration server use secure methods to supply the required information to the TLS certificate-authority server in order to obtain digital certificate(s).

One of the key points to keep in mind when selecting a secure method is that the configuration server must, under no circumstance, pass the RSA private key directly to the TLS certificate-authority server. The configuration server should pass only a proof of possession of the RSA private key to the TLS certificate-authority server.

In some cases, the TLS certificate-authority server is not on the isolated network. In these cases, it is strongly recommended that the connection between the configuration server and the TLS certificate-authority server be on a separate network interface from the interface the configuration server is using for the isolated configuration network.

Terminology

- CRL – certificate revocation list
- PKI – preshared key infrastructure

If no support for DN

If the configuration application server software or the enterprise infrastructure does not support a DN qualifier, the IT administrator can populate the system identifier in the OU field.

The TLS certificate authority server must generate certificates that are appropriately populated

The TLS certificate-authority is a separate server or is a capability integrated into the configuration server. Certificates generated for Intel AMT by the TLS certificate authority must have their fields appropriately populated. This includes:

- CN = fully qualified domain name (FQDN)
- UI = the device UUID
- DN = a subsystem identifier (Intel AMT System)

Manage Intel AMT certificates using a PKI

The best method of managing certificates for Intel AMT is through the use of commercial public-key infrastructure software. This may be limited to the use of a certificate server to generate certificates, or it may take a step further to include other PKI components such as a certificate revocation lists (CRL) published at a CRL distribution point, key management, reissuance, etc. These modules could be run from a separate certificate-management server or could be integrated into the configuration server.

From the standpoint of Intel AMT, one of the important aspects of managing certificates via a PKI is revocation of certificates. Certificates issued to Intel AMT may need to be revoked before they expire for two reasons:

- The private key has been compromised – someone other than the PC with Intel AMT also knows the private key
- The private key is no longer in possession of the PCs with Intel AMT. For example, it has been lost, corrupted in the flash storage area, or erased due to accident or error.

It is highly recommended that a revocation mechanism be in place to ensure that entities with malicious intent do not misuse compromised or lost certificates.

Configuration server should forget the secret and private keys after configuring them into Intel AMT systems

References to the PRNG secret key and RSA private key are generated during the configuration process. The configuration server should erase all such references as soon as those keys have been provisioned into the PCs.

If the configuration server does not erase those references, private or secret key values may remain in the configuration server's memory. Malicious programs or users could then generate a memory dump and search for the key values. System security can be breached if secret or private keys fall into the wrong hands.

Terminology

- 3PDS – third-party data store
- SDK – software development kit
- ISV – independent software vendor

Securing the memory space, not the data

Intel AMT controls access to the data storage area through HTTP digest authentication, TLS, and access control lists. Intel AMT does not provide encryption or other security for the third-party data in that memory. Encryption, privacy controls, or other protection for the data must be provided by the third-party application which stores the data in the protected, nonvolatile space.

Protect access to the data stored in the third-party data store

Applications that use the Intel AMT 3PDS should protect access to the data they store in that nonvolatile memory. To protect data, the applications should make use of the access-control features of the Intel AMT 3PDS manager. This will establish the first line of security for application data, and protect access to the data from other applications and malicious attackers.

Several commands are provided by the 3PDS manager to create access controls for stored data. These commands include a provision for group-access permissions. These commands are documented in the Intel AMT software development kit (SDK).

Encrypt sensitive data being stored in the third-party data store

ISVs are responsible for protecting the data stored in nonvolatile memory (3PDS) by their applications. The structure, meaning, and sensitivity of the data placed into the 3PDS are transparent to Intel AMT. Furthermore, Intel AMT does not ensure privacy of the specific data via encryption or other means. PCs with Intel AMT secure the memory space, and do not act directly upon the third-party data stored in that space.

If an ISV application uses the 3PDS to store sensitive data (such as keys, passwords, etc.), it is strongly recommended that the application(s) protect the stored data using encryption prior to storage. Encrypting sensitive data before storing it in the 3PDS significantly reduces the likelihood of an attacker obtaining the data.

Backup and restore data in the third-party data store

Application developers, who are developing applications that use the 3PDS, should keep a backup copy of the application ID, data-store configuration, and stored data. This will help IT administrators restore data in the event of data loss from the 3PDS. Intel AMT does not provide data backup services for 3PDS data.

Recommended extended security policies

Security policies are configured after device setup. These policies help IT administrators maintain the setup and configuration service policies. After setup and configuration, crucial security elements should be – or must be – updated to help maintain network security. These elements include time synchronization, Kerberos secret keys, each instance's network admin passwords, RSA keys and certificates, random-number generator (RNG) keys, and certificate revocation lists.

IT administrators must update:

- **Time synchronization.** IT administrators must periodically resynchronize the time and date of each Intel AMT instance, in order to ensure proper Kerberos operation. The hardware manufacturer or vendor should select a suitable default value in the factory to prevent IT administrators from having to tune this parameter in the enterprise.

IT administrators should frequently update:

- **Admin identity.** Enterprise policy may dictate that the network admin password for each Intel AMT instance be periodically updated.
- **RSA key pair and certificate.** Enterprise policy may dictate that the public key and corresponding certificate for each Intel AMT instance be periodically updated.
- **Kerberos key.** Enterprise policy usually dictates that the Kerberos secret key for each Intel AMT instance be periodically updated. This is analogous to a user updating a password.
- **RNG key.** Enterprise policy may dictate that the RNG secret key of each Intel AMT instance be periodically updated.
- **CRLs.** Enterprise policy often dictates that certificate revocation lists on PCs with Intel AMT be updated to match administrative CRLs.

For more information

For more information about security methodologies and technologies, refer to the security section of this guide.

Appendix B
Use Cases

Intel® AMT
Intel® Active Management Technology (Intel® AMT) is one aspect of the new hardware-based capabilities of Intel® vProTM technology

Terminology
In this guide, the term PC is used to refer to a PC with Intel AMT.

Introduction

Once Intel AMT is set up and configured, the PC can be remotely managed through Intel AMT capabilities from a centralized location, through a software-based management console. Although software-only solutions cannot usually communicate with PCs if the systems are powered off, their OS is unresponsive, hardware (such as a hard drive) has failed, or management agents are missing, Intel AMT allows you to remotely access even this segment of PCs.

This section describes some common uses and scenarios of Intel AMT features which may be helpful in proof-of-concept testing. Note that these are only the most popular scenarios which have proven valuable to many IT organizations that have already piloted Intel AMT. The scenarios are provided here as a starting point to help you identify and develop the use cases that will best suit your environment.

Management tools

Tools typically used for remotely managing PCs with Intel AMT include:

- **Third-party management software,** including a software-based management console that supports Intel vPro technology. This may require an upgrade to your management console. The console is used to perform remote configuration tasks on the PC.
- **Diagnostic tools,** which include a hardware diagnostic text-based tool set, a software diagnostic text-based tool set, and access to the event log stored in the nonvolatile memory of PCs with Intel vPro technology. These tools deliver help-desk procedures for remotely managing PCs, a process for identifying PCs with Intel vPro technology, and scripts for using the diagnostics text-based tool sets.
- **Remediation server,** which may be a Web-based repository for patches and OS updates.

This section describes some common uses of Intel AMT capabilities, which may be helpful in proof-of-concept testing. Note that these are only the most popular models which have proven valuable to many IT organizations that have already piloted Intel AMT. There are many other uses that may be appropriate for your IT environment, as well as more interesting uses that may be unique to your corporation.

Overview of common scenarios

Intel AMT provides IT administrators with new capabilities for remotely managing and improving security of PCs. These capabilities have been designed based on extensive research into the most critical IT problems. They offer IT organizations a new level of remote management that is available anytime, even if the PC is powered off, the OS is unresponsive, or management agents are disabled. As long as the PC is connected to a power source and plugged into the network, the capabilities are available to authorized IT technicians.

Some of the most common tasks for which IT organizations plan to use Intel AMT include:

- Discover and inventory PCs and their assets anytime
- Eliminate deskside visits for software and hardware problem resolution
- Monitor PCs more accurately with “always-available” alerting
- Update security software
- Install critical patches – even if PC power is off
- Automatically and continually check the presence of software agents
- Filter inbound and outbound network traffic and more quickly isolate compromised PCs
- Upgrade software or migrate a PC to a new OS
- Upgrade firmware remotely

The rest of this section describes some common uses of Intel AMT.

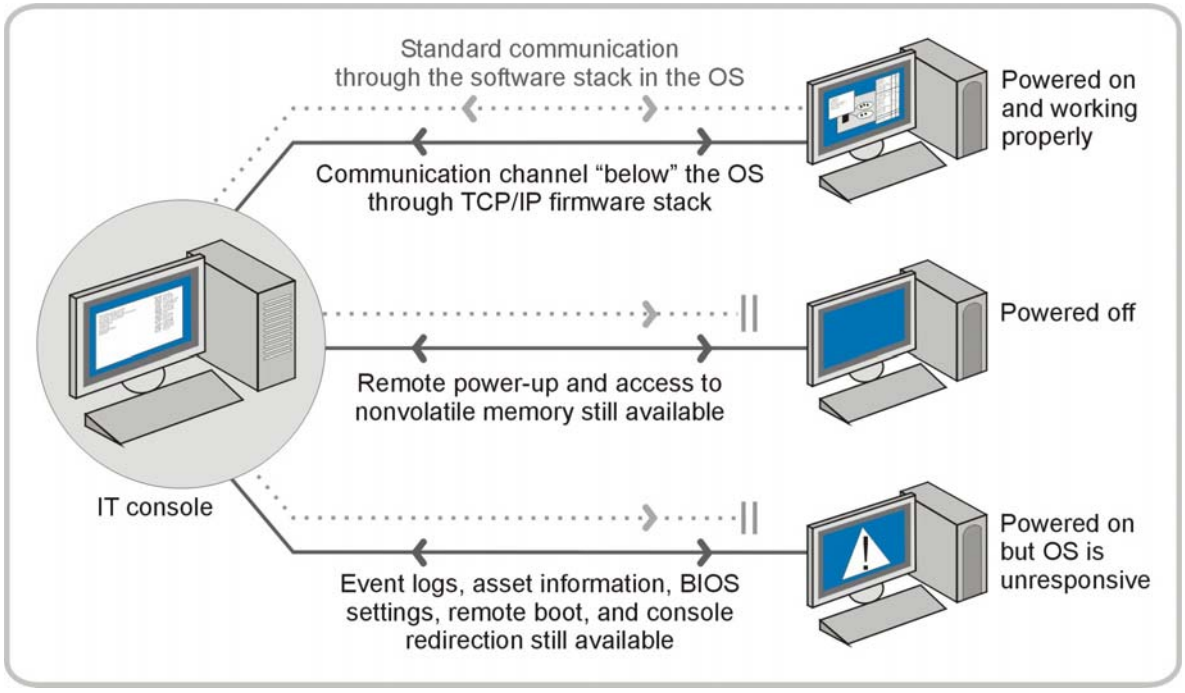

Figure B-1. Remote communication channel. The Intel AMT communication channel is available even if PC power is off, the OS is unresponsive, or management agents are missing.

Remote capabilities – always available

PCs with Intel AMT include a hardware-based remote communication channel that runs under or "outside" the OS. This channel uses the TCP/IP stack in the system's hardware and firmware, instead of the software stack in the OS. As long as the PC is connected to a power source and plugged into the network, the communication channel is available to authorized IT technicians (refer to Figure B-1, above).

With "always-available" communication, you can use Intel AMT capabilities anytime, even to access PCs that have traditionally been unavailable from the remote management console. You can now manage systems even if the PC is powered off, the OS is unresponsive, or management agents are compromised. You can communicate with the PC even if the OS or management agents have not yet been installed or hardware (such as a hard drive) has failed. Because the communication channel is hardware-based, it is also OS-agnostic, and independent of the type of OS being used.

For IT organizations, the improved availability of management capabilities allows you to perform more work off-hours and automate more tasks through third-party management software.

Discovery and asset inventory

One of the fundamental challenges facing IT administrators is discovering all devices on the network. PCs that can't be found can't be managed. Unmanaged PCs not only create a service problem for IT organizations, but these systems can fall dangerously out of compliance, creating security risks for the network. In addition, "missing" or inaccurately tracked assets can expose corporate officers to liabilities.

To help solve problems with asset tracking and inventories, Intel AMT provides several hardware-based capabilities that can be used to improve device discovery and asset tracking.

Discover PCs on the network anytime

PCs with Intel AMT can respond to an asset poll from authorized IT technicians even if system power is off, the OS is down, or management agents are not yet installed. This gives IT administrators greater visibility of the network as a whole.

Persistent UUID

The UUID is stored in persistent, tamper-resistant nonvolatile memory. This ID persists even across OS rebuilds and PC reconfigurations.

PCs with Intel AMT also include a universal unique identifier (UUID) stored in nonvolatile memory. Because the UUID is stored in tamper-resistant, persistent memory, it is available to authorized IT technicians, even if the PC is moved, the OS is rebuilt, software has been upgraded, or the hardware or software configuration has changed.

You can now poll a PC with Intel AMT and accurately identify the system anytime. This can significantly speed up PC discovery and help IT organizations track PCs more accurately through their life cycle, even in environments in which it has traditionally been difficult to access and find PCs.

Acquire the persistent hardware asset inventory

There are many conditions that prevent a PC from responding to an inventory poll of hardware assets. When a PC does not respond to a poll, costly manual inventories are often needed to ensure complete and accurate tracking of hardware, as well as compliance with government and other regulations.

Nonvolatile memory

Nonvolatile memory draws a tiny amount of current even when the PC is powered off, in order to keep hardware-asset information, event logs, and other information accessible at all times.

To help solve this problem, Intel AMT automatically stores critical hardware-asset information in persistent, nonvolatile memory. This information includes manufacturer, model, and other details for components, such as size of hard drive or component version number.

Hardware asset information is available to authorized IT technicians, even if the hard drive is replaced or the OS is rebuilt (refer to Figure B-2). In addition, the hardware asset information is updated each time the system runs through power-on self-test

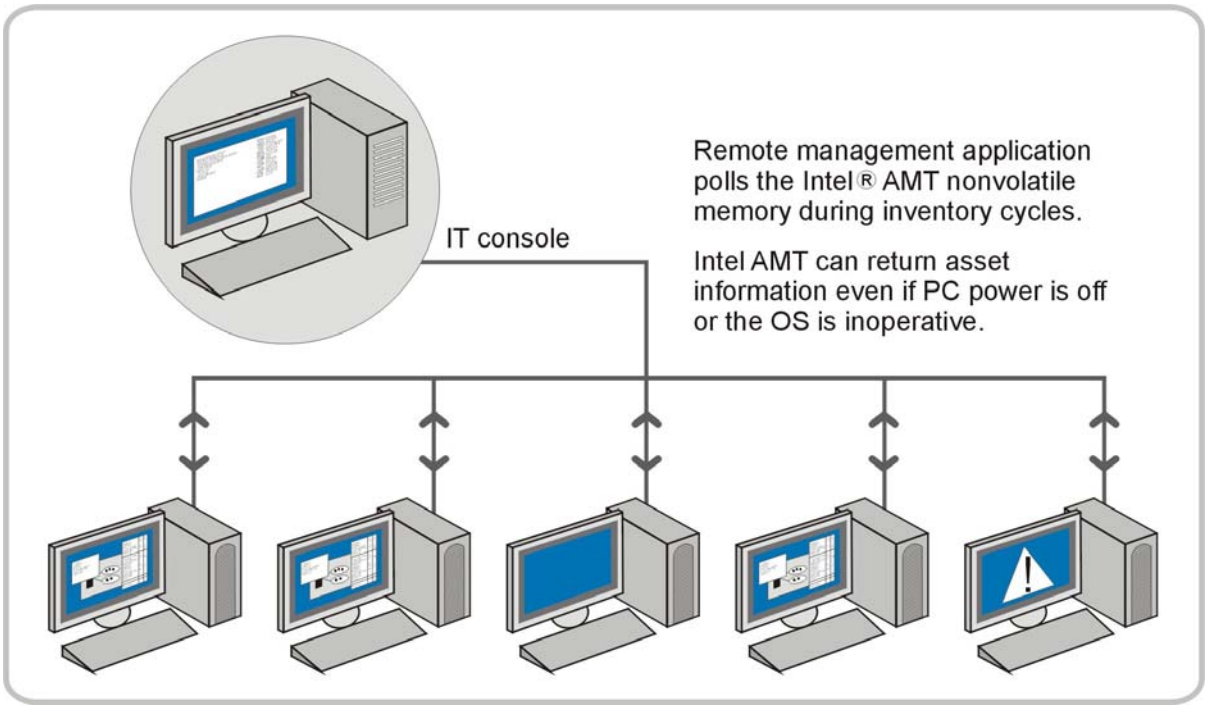

Figure B-2. Acquiring asset information anytime. Hardware asset information is persistent, and available even if PC power is off, hardware (such as a hard drive) has failed, the OS is unresponsive, or management agents are missing.

Access to hardware information anytime

Authorized IT technicians can upload hardware asset information from nonvolatile memory even before management agents are installed, if the OS is unavailable, if PC power is off, or if hardware has failed.

(POST). Because PCs are set up (including being powered up) before being accessed by management software, hardware asset information is available as soon as the PC completes its configuration process. You can now poll a PC and upload the hardware asset information anytime.

For example, an IT organization might deploy 5,000 new PCs with Intel AMT to user desks over a weekend. Because these PCs provide access to hardware asset information anytime, you can use your third-party management console to poll the network for the new PCs, and identify the hardware configurations, BIOS versions, and BIOS configuration settings remotely. You can then remotely power up the PCs and push the required management agents, software, and OS appropriate for those hardware configurations.

Access to persistent hardware information allows you to acquire more accurate inventory information regardless of PC power state or the availability of an OS. In turn, this can help you eliminate many manual inventory tasks, increase compliance, as well as improve maintenance contracts, inventories for field-replaceable units, and life-cycle planning.

Access a software asset inventory

Intel AMT allows authorized third-party vendors to store critical system information (such as software version numbers and .DAT file information) in persistent, nonvolatile memory. Authorized technicians can use this information to check for compliance anytime. If a polling agent discovers software that is out of date, the third-party management application can remotely power up the PC, push the update, then remotely return the PC to its previous power state. This can help IT administrators improve patch management, configuration updates, asset tracking, and many other processes.

Improving automation

Using third-party management software, hardware and software inventories can be streamlined, fully automated processes, even if PCs are powered off at the start of the inventory cycle.

For example, during a typical software inventory, IT technicians usually perform manual inventories for PCs that are powered off or whose management agents are missing. With Intel AMT, you can remotely discover PCs with Intel AMT, poll the systems for the software inventory stored in nonvolatile memory, and upload that information to the management console. You can then determine if any applications need updating or upgrading, maintenance, or other processes.

If a management agent has been accidentally (or deliberately) disabled or removed, you can even remotely power up the PC, push a new version of the agent to the PC, and perform a new software inventory – all without leaving the help desk.

"Always-available" access to third-party information, such as software asset information, can not only help IT organizations improve life-cycle management, but can help increase automation, improve the accuracy of software licensing and asset reporting, and increase compliance with government and other regulations.

Problem resolution

One of the most time-consuming tasks for IT organizations is problem resolution. Where other tasks, such as security updates, software upgrades, inventories, and backups can be planned and performed at scheduled intervals, problem resolution is often a constant, daily, time-consuming task with little or no predictability.

Problems that prevent a system from booting typically require at least one deskside visit to boot, troubleshoot, repair, and restore the PC. Hardware problems often require two visits: one to diagnose the problem, and a second visit to bring back and install the replacement part.

Software problems can often be resolved with a single deskside visit to boot, troubleshoot, and repair/rebuild the PC. However, even software problems can require a second deskside visit. For example, some applications (such as SAP, Oracle*, and business intelligence applications) are too complex for a standard technician to support. Problems related to these applications are often be escalated to a specialist who can perform more advanced diagnostics and resolution.

In addition, users in these industries don't usually have time to help troubleshoot or rebuild a problem PC, answer system prompts as directed by a remote technician, enter settings, or otherwise help with repair. In some industries, such as health care and public safety, interruptions may not only be inconvenient, but potentially dangerous.

To help improve remote problem resolution for both software and hardware problems, PCs with Intel AMT include several built-in, hardware-based capabilities. These capabilities can significantly reduce deskside visits traditionally required to resolve such problems, and can help improve the speed and accuracy of remote diagnoses and repair. The hardware-based capabilities include remote boot, console redirection, persistent event logs, persistent system information, and "always-available" alerting.

Resolve more software problems remotely

Software and OS problems can be caused by many conditions, such as a hard reboot while applications are running, a virus infection, or installation of unsupported printer drivers. Other corruption problems can be caused when a user downloads software that overwrites shared system files, or when someone tries to install an untested OS (for example, in addition to an approved OS, as a multiboot option).

* Other names and brands may be claimed as the property of others.

Remote problem resolution

The new remote problem-resolution capabilities of Intel AMT include remote/redirected boot, console redirection, persistent event logs, persistent hardware asset information, and "always-available" alerting.

Different IT organizations approach software issues in different ways, depending on their service environment. Some organizations use a swap-and-replace approach to get the user back up and working as quickly as possible. The swap-and-replace process shifts the problem to the service center and can create significant inventory problems. In addition, many problems could be relatively simple and less time-consuming to fix if you could just troubleshoot and repair the PC remotely. When a swap-and-replace approach is not used, many IT organizations escalate a problem through a series of increasingly skilled technicians, or perform a deskside visit to troubleshoot and repair the PC. These solutions are effective, but also often costly and time-consuming to both the IT organization and the user.

Changing the PC's boot device

Authorized technicians can now remotely change a PC's boot device to a different image, such as an image on a bootable CD at the help desk, a "diagnostics" server, local network storage, or another appropriate device.

Intel AMT now provides authorized technicians with several hardware-based remote diagnostics and repair capabilities. These include "always-available" alerting, access to preboot BIOS settings, remote/redirected boot, and console redirection. Help-desk technicians now have the tools they need to remotely troubleshoot, diagnose, and repair more software problems without leaving the help desk (refer to Figure B-3).

When a user calls the help desk with a problem, you can now reboot the PC from its own hard drive to reset its system state — without having to make a time-consuming visit to the desk. If this doesn't solve the problem, you can quickly and remotely change the PC's boot device to an image in another location.

Using console redirection, you can then watch from the management console as BIOS boots, drivers load, and the OS loads. This helps you remotely identify errors or problems in the boot process. If critical files (such as .DLL files) have been corrupted, you can push new files to the PC. You can also scan for viruses, update BIOS, clean up temporary files, restore user data, and perform other tasks as needed. You can then return local control of the system to the user – all without leaving the help desk.

Remote capabilities can help you boot, troubleshoot, diagnose, and repair more OS and application problems from the help desk. This can help you speed up diagnostics and repair, return PCs to the working environment more quickly, reduce labor costs, and improve user uptime.

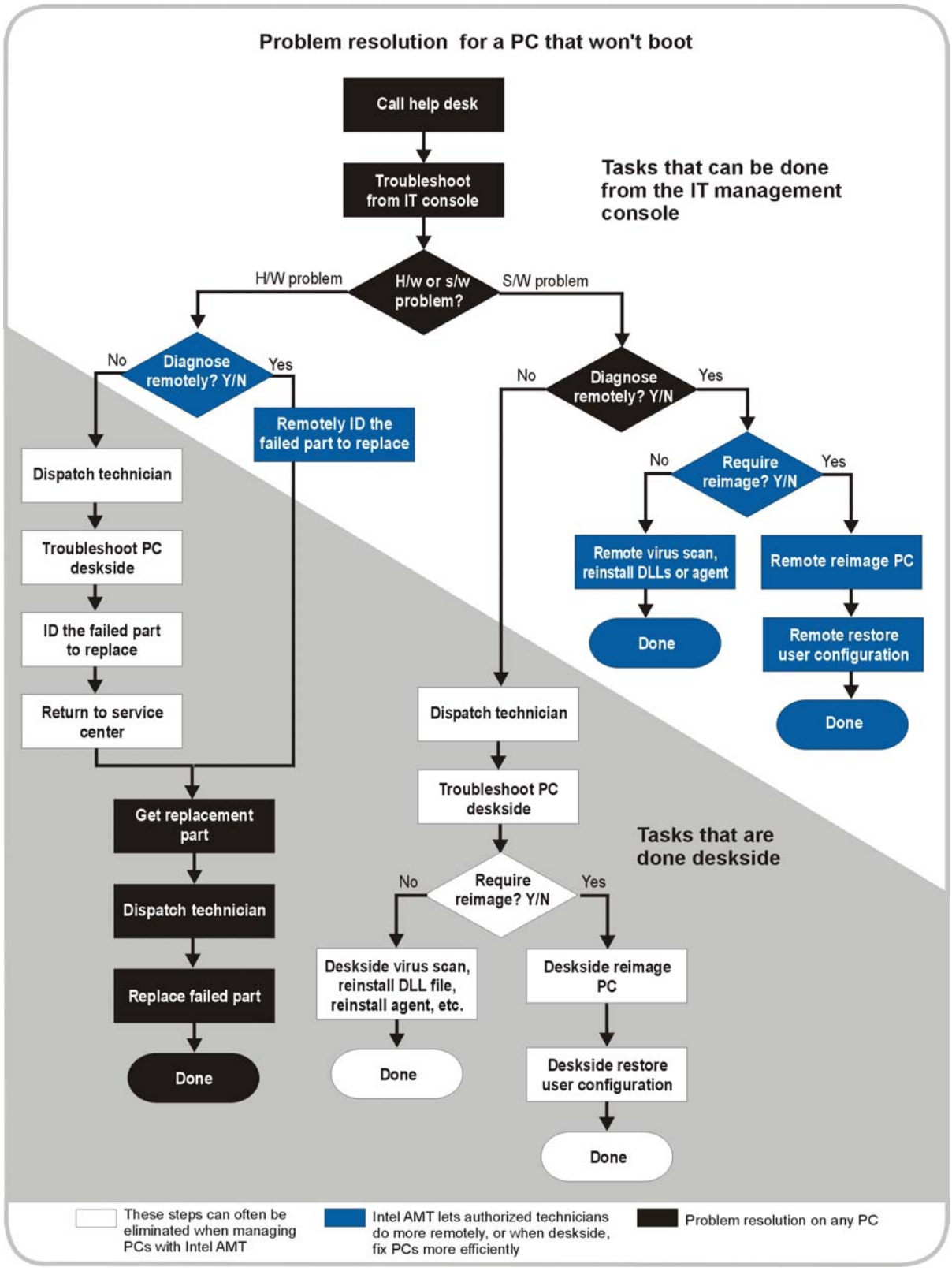

Figure B-3. Problem resolution for a PC that won't boot. Intel AMT can help IT administrators shift many tasks to the help desk, reducing deskside visits and improving user uptime.

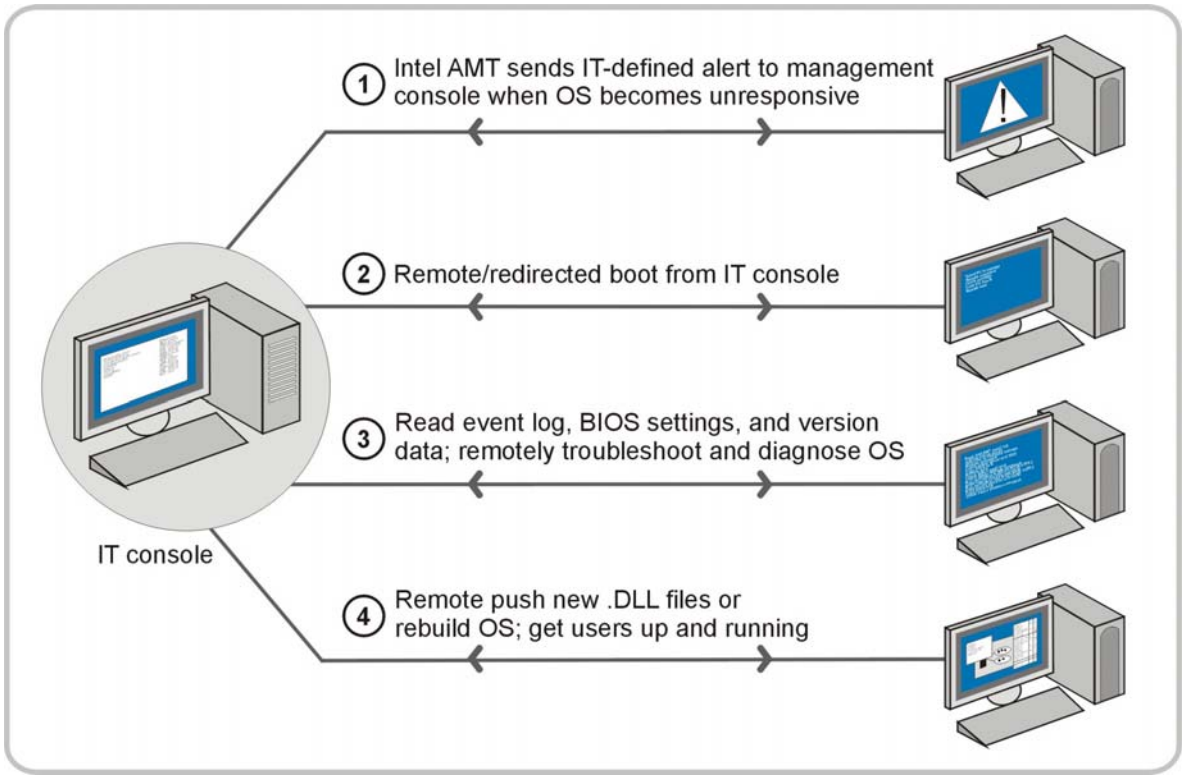

Figure B-4. Remotely rebuilding an OS. IT technicians can now troubleshoot, diagnose, and repair more software problems remotely, including reinstalling software, replacing missing .DLL files, and rebuilding an OS.

Rebuild OS remotely

Using the Intel AMT remote-boot and console-redirection capabilities, you can rebuild an OS remotely, directly from the help desk.

Remote rebuild to repair a corrupted OS

When an OS becomes unresponsive, it must sometimes be reinstalled (rebuilt). Typically, OS rebuilds are performed as a deskside service – a costly and time-consuming process. In contrast, when managing PCs with Intel AMT, you can now perform an OS rebuild remotely, without leaving the service center.

For example (refer to Figure B-4), a user might call the help desk about a PC that won't boot. In this case, you can use the remote boot capability of Intel AMT to try rebooting the PC from its own hard drive in order to reset the system state. If that fails, you could redirect the PC's boot device to a "clean" image on a remediation server. If the PC still doesn't boot, you could use the console-redirection capability to establish a remote troubleshooting session and watch as BIOS, drivers, and the OS attempt to load. In this scenario, you might realize that the OS has become inoperable, and the hard drive will need a full reimaging.

User intervention not required

When technicians can remotely diagnose and repair PCs, the user may no longer be required to help with the troubleshooting and rebuild process. Instead, the user could go to a meeting or work in some other area while the IT technician completes the rebuild.

You can then guide the PC through the rebuild process, using an OS image on a network share, remote server, or other appropriate device. You could remotely reinstall management agents, the user's applications, user data, and preferences, and return control of the PC to the user – all without leaving the help desk.

The ability to rebuild an OS remotely can help you save substantial time, eliminate many deskside visits traditionally required for a rebuild, and reduce labor costs. In turn, this can help you return a PC to the working environment more quickly and significantly increase user uptime.

Accurately diagnose hardware problems – even if the PC is down

Diagnosing and repairing a hardware problem traditionally requires two deskside visits: one for diagnostics and one to install the new part in the PC. Because authorized technicians now have access to preboot BIOS settings, persistent event logs, and hardware-asset information, you can identify the manufacturer and model of a failed hardware component without leaving the help desk — even if the PC is already down. This can allow a field technician to show up at the user site with the appropriate part to replace, eliminating the traditional deskside visit required for many initial diagnostics.

Reducing deskside visits

Access to persistent hardware information can significantly reduce the deskside visits traditionally required to identify hardware problems.

For example, traditionally when a hard drive fails, the PC is not available to the remote management console. Instead, a field technician is dispatched to the PC to diagnose the problem. The technician identifies the failed part, gets a new part from stores, and returns to the desk to install and verify the replacement component.

Now, when managing PCs with Intel AMT, you can use console redirection to watch as BIOS loads, and note the "missing" hard drive (or other component). You can then access the persistent hardware information of the Intel AMT nonvolatile memory, and note the manufacturer, model, and size of the failed hard drive. The field technician can then be dispatched to the user desk with the correct hard drive in hand.

In addition, because failed components can be accurately identified before being taken the user desk, you could image the new drive at the service center. When the field technician installs the new component, the system is quickly ready to go, without a rebuild required over the network. This can save both the IT department and the user significant time. Especially in time-critical industries, such as public safety and health care, this type of service improvement can have a significant impact that goes beyond simply improving hardware repair.

Access to preboot BIOS settings

Using the Intel AMT access to preboot BIOS settings, IT technicians can now access and change the settings from the service center.

Updating BIOS settings

Often a help desk will receive a request to change the boot device in a PC. This typically requires a deskside visit to change the boot order in BIOS. However, because Intel AMT allows authorized technicians to access preboot BIOS settings, you can now perform this service remotely, without leaving the help desk.

For example, perhaps a user wants to temporarily boot a PC from a bootable CD instead of the hard drive. Using preboot access to BIOS settings, you can now update the BIOS settings and change the boot order – without leaving the service center. The traditional deskside visit can be eliminated, and the ticket closed with minimal resources expended. This type of task could even be performed as an automated, off-hours process, triggered by the service ticket. When the user came in the next day, the system would already be updated and ready to boot from CD.

"Always-available" alerting

Because PCs with Intel AMT can communicate with the management console anytime, they can also send alerts anytime. Alert events can include simple network management protocol (SNMP) traps, Microsoft Windows* management instrumentation (WMI) events, and third-party management software events. IT-defined events can now be received, even if PC power is off, hardware has failed, the OS is unresponsive, or management agents are missing.

Confirm critical events

Some IT organizations rely on management software to log events, but need to be able to confirm events when hardware fails or the OS becomes unresponsive. In this case, the persistent Intel AMT event log can be used to confirm suspected events.

For example, management software might notify you that fan speeds have slowed below established metrics, and the next day, the hard drive fails. Looking at the event log in management software, you may suspect that the cause of the hard-drive failure is actually a failed fan. In this case, you can access the persistent Intel AMT event log and confirm that fan speeds slowed and temperatures spiked just before the hard-drive failed. You could then attempt to reboot the PC and watch as BIOS loads, to note the "missing" (failed) hard drive.

Event log in nonvolatile memory

PCs with Intel AMT store an event log in nonvolatile memory. This log is available to authorized technicians anytime, even if PC power is off or the OS is unresponsive.

By using the Intel AMT event log to confirm in more detail the management-software log – even though the PC is now unresponsive – you can more accurately identify the parts that might need replacing or repair. In this case, confirmation that both the fan and hard drive have failed can help increase your confidence in dispatching a field technician to the site with all the correct replacement parts needed to repair the PC upon the first visit.

Acquire the event log even if management agents are not installed

Some business environments do not allow – typically for security reasons – installation of the software agents that collect events and send them to the management console. This has traditionally been a difficult challenge for IT organizations to resolve.

Event log

All PC events are logged in the Intel AMT event log. IT administrators can define the events that will also be sent to the management console as alerts.

Because Intel AMT logs events regardless of the presence of management agents, you can now acquire event logs and receive notifications even if such agents are not installed. Such events could include application hangs, OS lock-ups, temperatures above defined thresholds, hard-disk spin-up speeds below expected thresholds, and so on. Acquiring such information remotely can help IT organizations achieve greater visibility of PCs that have traditionally been difficult to monitor.

For example, you can poll a PC after-hours for its event log, upload the log, and correlate critical events to metrics stored in a database. This can help you identify potential problems before they become serious enough to bring down a system. Most importantly, because the event log is OS-agnostic and independent of the presence of management agents, the information is available to authorized technicians anytime.

Performance monitoring

Maintenance tasks, such as performance monitoring and optimization, can be performed off-hours, using a combination of Intel AMT capabilities, such as remote power-up, access to persistent event logs, and console redirection.

Monitor PC performance

Some IT organizations conduct performance analysis to help identify potential problems before they bring a system down. Other organizations use performance analysis as a tool for infrastructure modeling, in order to identify cause-and-effect processes and help the company optimize resources (refer to Figure B-5 on the next page). These IT organizations can take advantage of the persistent Intel AMT event log, as well as the "always available" alerting to identify specific events that may affect performance. Because the event log is stored in tamper-resistant, nonvolatile memory, you can access the event log even if the PC itself is powered off or unresponsive.

For example, if a user calls the help desk because the PC seems slow, you could notify the user that diagnostics will be performed after-hours, when they won't interfere with the user's work. After the user goes home, you can remotely power up the PC and run analysis tools to establish a baseline for performance. You can then monitor the PC the next day, while the user is working, to identify potential problems. This could include monitoring hard-disk fragmentation, hard-disk spin-up speed, the number of background processes running at any given time, temperature zones in the PC, fan speeds, and so on.

If the problem is with the number of applications or background processes running at the same time, you might begin terminating background processes that are interfering with the user's work, or might decide to add more RAM to the system. If the problem is hard-disk utilization, you could determine if the hard drive needs to be defragmented, repaired, or replaced, before the drive fails completely, and user productivity is severely interrupted.

Because event management is based in hardware and firmware, event information is available independent of the type of OS, and even if the PC does not have a management agent installed. This gives IT organizations more flexibility in monitoring, modeling, analyzing events.

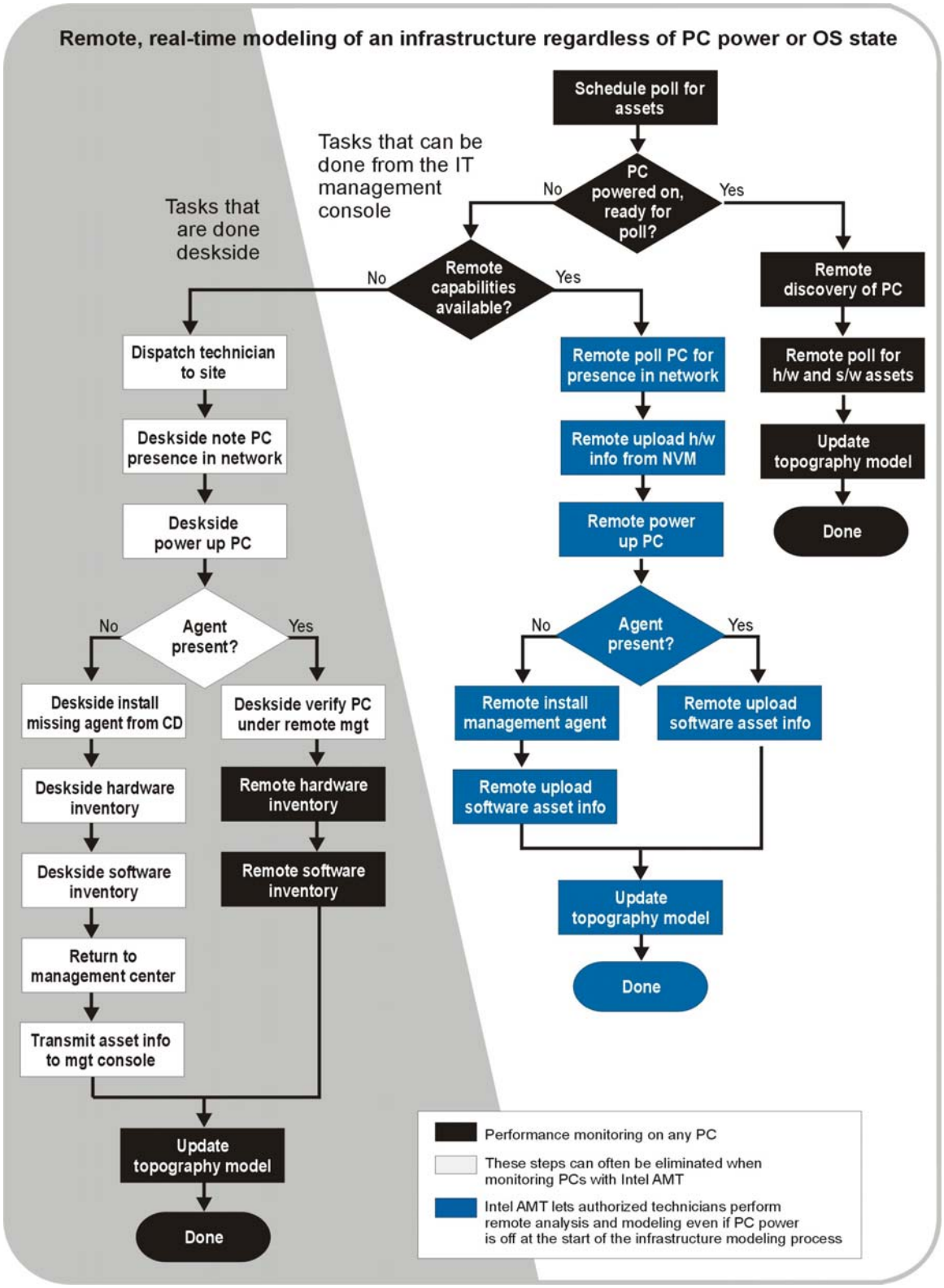

Figure B-5. Monitoring the enterprise infrastructure. Intel AMT can improve real-time visibility of the enterprise infrastructure, helping technicians identify PCs that may need maintenance or other attention.

System Defense

Intel AMT delivers a new category of capabilities called system defense, including agent presence and network outbreak containment. These capabilities provide hardware-based timers for checking the presence of security agents, hardware-based filters for inbound and outbound network traffic, and isolation circuitry.

Security

One of the most critical challenges in managing PCs is security. Today, many PCs are inaccessible from the management console for remote security updates, such as critical patches and software upgrades. Other challenges include making sure security agents remain present and working properly, and being able to quarantine PCs that may have been compromised.

To meet these security challenges, PCs with Intel AMT include several hardware-based capabilities, such as remote power up, agent presence, and network outbreak containment. The built-in capabilities can help IT administrators update systems faster, be notified quickly when a software agent is compromised or disabled, and isolate PCs faster during malicious attacks and other events.

Update security software off-hours

Security updates are often challenging to complete for many reasons. First, many PCs are powered off at the start of the update cycle. In large enterprises, where 10% to 20% of PCs may be off at any given point in time, 100% saturation of an environment may never be achieved. A second critical challenge is that users can refuse to accept an update because it might interfere with their work. In addition, PCs that are already compromised may not be found during a poll, and may be missed in the update cycle, opening dangerous vulnerabilities into the network.

Remote power-up

The remote power-up capability allows authorized IT technicians to power up, power down, power cycle, and reset PC from the service center.

To help improve security updates, Intel AMT provides a remote power-up capability for authorized technicians. This capability allows you to power up, power down, power cycle, and reset systems remotely. You can now remotely update PCs even if power is off at the start of the update cycle. You no longer needs to remind users to leave their systems powered up when they leave work for the day. Instead, updates can be performed after hours, on weekends and holidays, independent of the PC's initial power state.

For example, an IT organization might schedule an automated security update for late evening, after workers have left for the day. In this scenario, the third-party management application could poll PCs with Intel AMT on the network, identify their power state, and begin the automated update for systems that are already powered on. A second automated process could begin powering up PCs that are off, install the update, and then return those systems to the state in which users left them: on, off, hibernating, or sleeping.

Remote power-up

The remote power-up capability allows IT administrators to schedule more updates off-hours, automate more security processes, and streamline many security tasks, improving compliance and reducing the window of vulnerability.

The remote power-up capability helps IT administrators speed up security updates, achieve improved compliance, and reduce the window of vulnerability for systems that are typically powered off during the update cycle. In addition, IT administrators can now streamline and automate more tasks, and perform more work off-hours, when it won't interrupt users.

Remotely Install critical patches

One of the primary security challenges currently facing IT organizations is being able to deploy a critical patch quickly and thoroughly to a large environment. Typically, when a critical vulnerability is announced, IT administrators call, email, or otherwise notify site administrators to begin an immediate patch process. Technicians are then dispatched to go from desk to desk, powering up PCs from a bootable CD.

The technicians make sure each PC's security agent is not compromised, install the patch, and watch to make sure the patch completes successfully, before the PC is allowed network access again. In extreme cases, even users may be asked to help locate and power up PCs that are powered off during an emergency, in order to patch those systems. In large environments, such manual processes are not only time-consuming, they can extend the network's window of vulnerability to a threat.

Remotely installing a patch – even if PC power is off

Because Intel AMT provides a remote power-up capability, IT administrators can now remotely power up PCs to receive a critical patch.

For example, you can send an email announcement to all users notifying them of the patch, then begin patching all PCs that are powered on. You can then poll PCs for their power state, identify PCs that are powered off, and power up the systems. You can then remotely push the patch and, when finished, return the PC to its previous power state: on, off, hibernating, or sleeping. Most importantly, this can be done from the service center, without a deskside visit.

The remote power-up capability represents a significant improvement, not just in the time required to achieve patch saturation (refer to Figure B-6 on the next page), but in the virtual elimination of the deskside visits traditionally required to power on systems to receive a critical patch (refer to Figure B-7 on the following page). This could be a key capability in certain environments, such as health-care, pharmaceutical research, and other industries where privacy is critical and you may not have immediate access to PCs in order to update or patch the system.

[1] **Source:** IT outsourcer evaluations of Intel AMT, as reported in various white papers, including: "Improving IT Services and Increasing User Uptime with Intel® vPro™ Technology," 2006, Intel; "Improving Asset Inventories and Reducing IT Costs with Intel® vPro™ Technology," 2006, Intel; and "Reducing Manual Processes with Improved Remote Security, Inventory, and Problem-Resolution," 2006, Intel. To read these and other industry evaluations of Intel AMT, visit the Intel Web site.

From a management viewpoint...

In some cases, IT administrators do not install software agents because, from a management standpoint, the agents themselves require a support framework to stay active. This creates yet another layer of infrastructure for administrators to manage.

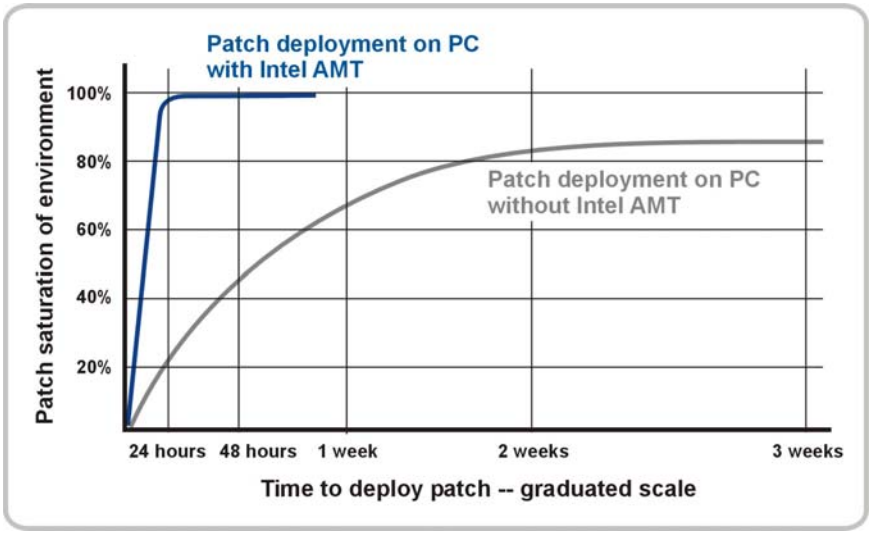

Figure B-6. Deploying OS patches to 30,000 PCs. Based on data from various third-party evaluations of the Intel AMT remote power-up capability, IT organizations could use the capability with third-party management software to deploy patches to 20,000 PCs potentially within 24 hours.[1]

Patching PCs that don't have software agents

In some corporate areas, IT organizations do not install software security or management agents on the PCs. Typically this is for security reasons since, from a security standpoint, every agent compromises system security through its communication port. Hackers, viruses, and other threats can use those ports to compromise a system, or subsequently, to compromise a network. In these environments, technicians typically make a deskside visit to install OS patches, update security software, or perform other security tasks.

Because PCs with Intel AMT include the remote/redirected-boot and console-redirection capabilities, you can now patch even these PCs from the service center. For example, you could remotely change the boot device of the PC to an "image" server. You could then use console redirection to remotely install the OS patch. This could not only help reduce deskside visits to "open" PCs, but automate what has traditionally been a manual process, and help improve both PC security and stability.

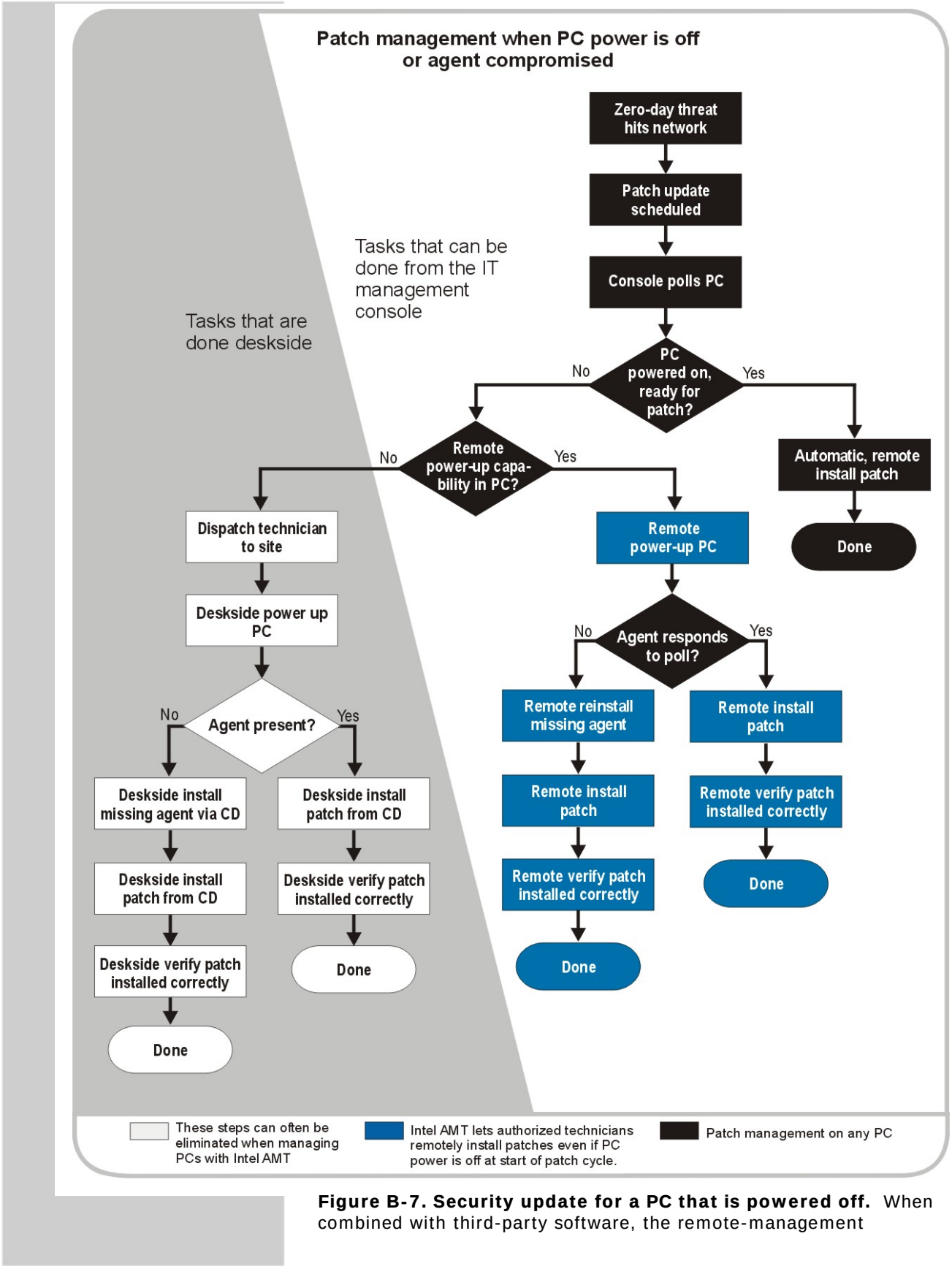

Figure B-7. Security update for a PC that is powered off. When combined with third-party software, the remote-management

capabilities could help eliminate most of the deskside visits traditionally required for security updates and patches.

Mass shut-down during malicious attacks

The remote power-up capability provides IT administrators with a new level of control for many tasks. For example, an administrator could use the capability to power down machines during emergencies caused by malicious attacks and other events. This would isolate PCs and help prevent the spread of the threat. Once a solution has been found or the attack is over, the administrator can remotely power up PCs again, install the security update or OS patch, and return PCs to the production network.

Automated, continual checking for agents

Hardware-based timers

Intel AMT allows software applications to register with the system defense capabilities and take advantage of hardware-based timers to check in at regular intervals. Intel AMT can now quickly – and accurately – notify the management console of a "miss" by a registered software agent.

One of the challenges IT administrators face in ensuring compliance is that hackers, viruses, worms, or other malicious attacks disable or remove management, security, or other software agents. Once management agents are removed, PCs are often unavailable to the remote management console and vulnerable to further attack. Compounding the problem is that users often accidentally – or deliberately – disable or remove software agents in order to keep virus scans and other IT processes from intruding on productivity, with the result that PCs can fall dangerously out of compliance.

Traditionally, IT organizations have used serial polling to verify the presence of security agents (or other business-critical applications). In contrast, PCs with Intel AMT use a regular, programmable "heartbeat" presence check, which is built into the Intel® Management Engine. The heartbeat uses a "watchdog" timer so third-party software can check in with the management engine at programmable, one-second intervals, to confirm that the agent is still active.

Each time an agent checks in, it resets its timer. If an agent hasn't checked in before the timer goes off, the agent is presumed removed, tampered with, or disabled. The management engine then automatically and immediately logs the alert and notifies (if specified) the IT console.

Once notified, you can automatically begin an integrity check of the compromised agent. If the agent is turned off but still present and viable, you can remotely and automatically push an event to the problem PC and start the agent back up. If the agent has been compromised by a virus or other malicious attack, you can use other Intel AMT system defense capabilities to remotely quarantine the system until it can be remediated, according to corporate policies.

With hardware-based heartbeats, IT administrators no longer need to wait for multiple polls to identify a potential problem. The PC itself helps improve the reliability of presence checks and reduce the window of software vulnerability. And, because of the "always-available" alerting and remote power-up capability, the entire process of checking and reinstalling missing agents can be automated, improving compliance further and saving additional resources.

Filtering inbound and outbound network traffic

PCs with Intel AMT include programmable hardware filters for examining the behavior of inbound and outbound network traffic. These filters examine packets before they are passed from the hardware to the OS, or before packets are passed from the software stack out to the network. The filters examine the source, destination, and port address within the packet headers.

Network outbreak containment

The NOC capability allows an administrator to rate-limit network traffic to a PC, restrict the PC's communications to specific ports, or fully quarantine a PC from the network, based on IT-defined policies.

Because the filters are programmable, management software can define events triggered by proscribed packet behavior. Such events could be to log an alert, send an alert to the IT console, or trip the threat-containment isolation circuitry (network outbreak containment, or NOC). The NOC capability allows IT administrators to set a rate-limit for network traffic to and from that PC, restrict communication to specific ports (such as remediation ports), or fully quarantine the system by disconnecting the network data path to and from the OS. You could then have more time to investigate a potential threat.

For example, you might suspect that PCs on a subnet have become compromised. Using a third-party application, you can employ the hardware-based filters to check the network traffic to and from a group of these machines. If a filter triggers, the management application could log the event, send you an immediate alert, and restrict the PC to communication with an isolated remediation server.

Because the PC includes other Intel AMT capabilities, you can still communicate with the underlying hardware of the PC through the built-in TCP/IP firmware stack. You can then use remediation ports and remediation software to correct the problem and bring the PC back into the enterprise network.

In addition, because only OS network communication is switched off, user applications (such as word processing and spreadsheets) can remain enabled, so users can continue to work, even while threats are being investigated and resolved.

Upgrades and maintenance

Intel AMT provides IT organizations with new tools to perform a variety of upgrade and maintenance tasks from the service center. With the remote power-up capability and “always-available” asset information, UUID, and configuration information, you can perform more work when it does not interfere with user productivity. This includes software upgrades, OS migrations, firmware updates, back-ups, disk defragmentation, and performance evaluations.

Upgrade software and migrate an OS – without leaving the service center

Because Intel AMT includes a remote power-up capability, as well as access to persistent system information, you can automate more upgrade and migration processes.

When new PCs are deployed to an environment, you can use the third-party management console to poll the network for the new PCs and identify the PC’s configuration — including BIOS settings and firmware version information — even before management agents are installed. You can remotely power up the systems, push the required management agents to the new PC, and perform the rest of the enterprise build (such as installing drivers, the OS, and user applications) using the typical management process.

When PCs require application upgrades or migration to a new OS, you can remotely inventory the hardware and software assets on the system from information stored in the persistent, nonvolatile memory. You can then accurately identify the PC’s configuration, identify PCs that require a software upgrade, and push the new version of software. With the remote power-up capability, this entire process can be automated and performed off-hours. This could save IT organizations a significant amount of time, improving efficiencies and reducing the number of technicians required to perform an upgrade or OS migration.

Typical cost of a BIOS update

An OS migration for 5,000 PCs could require over 400 staff-hours just to update the BIOS, in order to ready the PCs for the remote rebuild. If technician rates are $70/hour, that is almost $30,000 spent solely for BIOS updates.

Remotely updating firmware for OS migrations

IT administrators have few tools today to automatically track and update BIOS. Because of this, few IT organizations update BIOS on a regular basis. Instead, when a BIOS corruption occurs or the PC is being serviced for some other reason, technicians typically install the new files manually while making the deskside service visit. When BIOS must be updated as part of an OS migration, even though the deskside task typically takes only about 5 minutes per PC, in a large enterprise, the cumulative time spent to update all systems can be substantial.

Along with other critical system information, Intel AMT provides authorized technicians with access to preboot BIOS settings and version information. This allows you to remotely view and change system BIOS settings from a remote console.

For example, you can poll PCs with Intel AMT, upload BIOS version information and settings, and identify PCs that require a firmware update. You can then change BIOS settings as required, or push a full firmware update to the system.

With remote access to the settings, this process can also be automated and performed as part of a regular maintenance cycle, instead of being performed on an ad-hoc basis during problem resolution. This can help increase the overall stability of the user's system and help prevent many potential issues from bringing down the PC.

Performance metrics

Metrics that could indicate a particular level of system utilization could include memory capacity, RAM usage, temperature levels around a processor, and fan speeds.

Distributed computing

Some organizations may find that Intel AMT enables new and interesting usage models, especially in environments where clients do not allow installation of software agents.

For example, many organizations are beginning to look at distributed computing usage models. In such a scenario, jobs that require intense processing are distributed over multiple existing resources that, during certain times (such as after-hours or on weekends), are being underutilized.

With the Intel AMT remote discovery and persistent event logs, a third-party application could identify the power state and base metrics of such PCs without powering them up. This would allow the application to dynamically determine which machines are under load, and which could be assigned some of the distributed work.

Summary

The built-in capabilities of Intel AMT can significantly improve many management and security processes, such as security updates, software and firmware upgrades, OS migrations, inventories, and problem resolution. These new capabilities can help IT organizations streamline and automate more processes, improving efficiencies for many tasks. In addition, when managing PCs with Intel AMT, you can eliminate many of the traditional deskside visits required to diagnose problems, and shorten repair and remediation times. This will help IT organizations minimize interruptions to daily business and improve user uptime. Overall, Intel AMT can help IT organizations reduce service costs and shift more toward becoming an enterprise asset instead of a cost center.

For more information

For information about how many industry-leading software vendors are taking advantage of the new hardware-based Intel AMT capabilities, refer to the Intel Web site. The site includes white papers, case studies, and solution briefs featuring many third-party software solutions.

In addition, the site includes several IT outsourcer evaluations of Intel AMT, as reported in various white papers, including "Improving IT Services and Increasing User Uptime with Intel® vPro™ Technology," 2006, Intel; "Improving Asset Inventories and Reducing IT Costs with Intel® vPro™ Technology," 2006, Intel; and "Reducing Manual Processes with Improved Remote Security, Inventory, and Problem-Resolution," 2006, Intel.

The deployment planning section of this guide explains how to plan and test Intel AMT capabilities for your environment.

Appendix C
Deployment Planning

Intel® AMT
Intel® Active Management Technology (Intel® AMT) is one aspect of the new hardware-based capabilities of Intel® vPro™ technology

Introduction

Before planning to deploy a new technology, IT managers need to know how the technology would fit into their business environment. How is security handled for out-of-band communication? How can the technology solve critical IT problems?

This section explains the general deployment-planning process, from analyzing business needs to conducting proof-of-concept and pilot tests. This section is intended to help you evaluate the benefits of Intel AMT for your business environment.

Deployment planning and technology evaluation

Deployment planning should start with an analysis of business objectives and the challenges being faced. Deployment planning follows these general steps (refer to Figure C-1):

1. Analyze business needs.
2. Identify IT management issues and challenges. These could include a need to reduce deskside visits or service calls, improve compliance, and increase the accuracy of asset inventories.
3. Map problems and challenges to usage models that can be tested in a lab environment.
4. Set up, execute, and evaluate proof-of-concept (POC) testing to verify that proposed solutions can address issues and challenges.
5. Conduct an early-adoption pilot, to modify POC usage models for your specific environment, develop internal processes for using the technology in your business, and evaluate the technology benefits in a real-world setting.

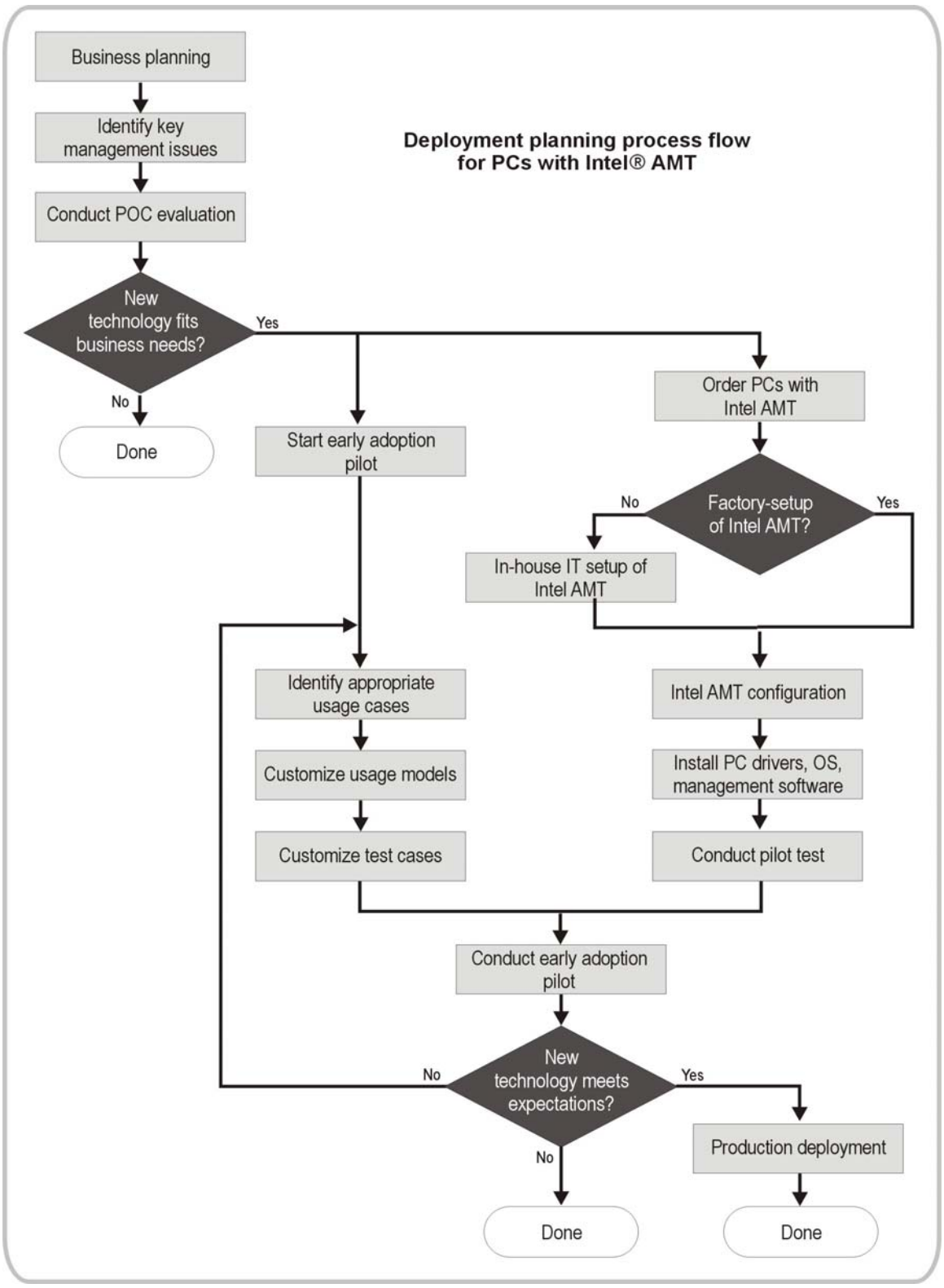

Figure C-1. Process flow for deployment planning. Deployment planning helps connect business needs to usage models, and more accurately predict how technology can improve business practices.

Based on results from the pilot test, corporate officers can make an informed decision about whether this new technology will be supportable, scalable, and deliver the needed return on investment, in order to justify its deployment in a large scale in the production environment.

Analyze business needs

Business planning helps you identify business needs and analyze the consequences of unresolved issues, such as lost business opportunities, unmet customer expectations, or increased operational costs for IT services. The point of analyzing business needs is to identify ways to reduce such costs or improve operational excellence.

When planning investigation or deployment of a new technology that could help reduce costs or improve services, businesses should take many factors into consideration. These include the cost of new hardware, the cost of associated equipment, human resources required, the complexity (or simplicity) of new processes, the cost and time required for software upgrades, the potential savings delivered by the new technology. These factors can be analyzed to estimate the potential benefit of the new technology.

Businesses should also consider how the new technology will be rolled out. Most businesses have many legacy systems and technologies in their environments. Managing a mixed environment presents challenges that, although not unusual, do require resource planning. Businesses need to take the required upgrade cycles into account when setting expectations for a transition to a new technology.

Identify IT manageability issues and challenges

Identifying the issues facing your IT department can also help you understand how management capabilities can resolve those challenges. There are many articles and resources available to help businesses analyze IT issues. You should also look at areas in which your IT department is spending most of its resources to keep technology running. In addition, look at other, less obvious areas in which a solution could substantially reduce spending.

Once you have identified the key issues and areas where a solution could save resources, those areas can be mapped to usage models for proof-of-concept testing.

"Always-available" capabilities

Intel AMT capabilities are available as long as the PC is connected to a power source and plugged into the network.

3PDS

Nonvolatile memory is divided into three areas. One of the areas – the 3PDS, or third-party data store – can be used by third-party vendors to write/store data specific to their applications. For example, a third-party vendor could store software version numbers, an update history, or configuration information in the 3PDS.

Managed environment

A well-managed environment is a well-secured environment. Intel AMT capabilities help you explore new usage models that can help improve the managed state and security of your PCs.

Map manageability challenges to usage models

Once you have identified the most important challenges faced by your IT organization, you should map those challenges to the capabilities of Intel AMT. These usage models include:

- **Asset discovery.** This is the ability to discover PCs on the network. With "always-available" communication capabilities, PCs with Intel AMT can respond to polling processes anytime, even if the PC is powered off, the OS is inoperative, or management agents are missing.
- **Hardware/software inventory.** Inventory of hardware and assets is required for regulatory compliance. An incomplete asset inventory leads overpurchasing of assets, inefficient redistribution of unused or underutilized assets, and exposure of the corporation to liabilities from inaccurate asset reporting. Inaccurate asset information also poses a security threat because IT organizations need to know which assets require securing. Unknown or unmanaged assets can present critical vulnerabilities. PCs with Intel AMT provide access to hardware asset information (updated each time power-on self-test runs) and access to information in the third-party data store (3PDS) anytime, even if an OS is unresponsive or management agents are missing.
- **Problem resolution.** This is the ability to remotely boot, troubleshoot, repair, and rebuild systems – without leaving the service center or help desk. Intel AMT provides new mechanisms to remote boot, control, diagnose, and repair a PC, even if the OS is inoperative. With access to persistent hardware asset information, a technician can also more accurately identify a failed hardware component (such as a hard drive or video card) without leaving the help desk.
- **Security updates and patch management.** One of the biggest problems today with security updates and patch deployment is updating PCs that are powered off. PCs with Intel AMT give IT administrators a remote power-up capability that is secured with HTTP digest authentication and TLS. This can substantially reduce manual updates and patch deployments.
- **Missing agents.** One of the main problems with remote management is keeping software agents present and operative. PCs with Intel AMT include hardware-based timers so software applications and agents can check in at IT-defined intervals. Since any miss indicates a problem, IT no longer has to wait for multiple polls to identify a potential problem.

- **Identifying threats and isolating PCs.** During a particularly malicious attack, IT administrators often need to perform an emergency mass shut-down. This usually requires teams of technicians (and users) going desk to desk to power down machines until a resolution is developed or the attack is over. The remote power-up capability of Intel AMT also allows technicians to perform an emergency mass shut-down remotely, even if systems are already compromised. These PCs also include circuitry (network outbreak containment) that allows IT administrators to set policy-based rate-limits and perform policy-based quarantines for PCs that may already be infected.
- **Event notification.** In today's global business environment, IT processes are often executed around-the-clock. In addition, to reduce user downtime, IT technicians need to know as issues arise, before they bring a system down. PCs with Intel AMT can send alerts and platform event traps anytime, even if software or hardware has failed. This allows IT technicians to be quickly notified when issues occur, and respond more quickly to both software and hardware problems.

Usage models for many of these IT challenges are described in detail later in this guide.

Conducting a POC evaluation

A proof of concept (POC) project is a check of how well the Intel AMT solution fits into your environment. These evaluations should not last more then three or four weeks, nor involve much customization of usage models or management software. They usually require three to five experienced IT engineering and business professionals, and two or three PCs with Intel AMT.

The purpose of a POC evaluation is simply to give you a basic understanding of how Intel AMT can deliver the new management and security capabilities in a secure and reliable manner. POCs are not designed to prove that Intel AMT works, but to help you evaluate how it works in your service environment, and help you identify challenges and remove barriers with regards to PC management. They are a relatively inexpensive way to form an opinion about a new technology before planning or investing in a corporate-wide deployment. In addition, POC projects make it easier for businesses to deploy and adopt new technologies in the most effective manner.

POC feedback also helps Intel

POC projects also help Intel by allowing service providers and businesses to provide valuable feedback on capabilities and new usage models. This can help Intel improve designs and build even more robust features in future versions of the technology.

* Other names and brands may be claimed as the property of others.

General steps for a POC evaluation

A POC usually follows these general steps:

1. **Assemble a POC team.** This is usually three to five experienced engineering and business personnel. Time commitment is usually short, no more than four weeks after equipment is in place.
2. **Define business objectives and the POC plan.** The POC team must have clearly defined objectives of the business problems they are trying to solve. They should develop test plans according to the use cases being tested. Test cases should be short and cover one business problem at a time. They should have quantifiable metrics so that you can measure the effectiveness of the technology.
3. **Acquire test equipment and build the test environment.** Acquire two to three PCs with Intel AMT, management software, and any additional necessary software, such as Microsoft Active Directory*. You can then build the test environment in an isolated lab with only the components under test. An isolated environment helps teams eliminate distractions, and focus on specific IT issues and how Intel AMT can help solve those problems.
4. **Test use cases and collect data.** Pay attention to how you should integrate Intel AMT with management software.
5. **Analysis and summary.** Summarize the results of the POC evaluation in order to identify the potential benefits of deployment of Intel AMT in the production network. This will also help you identify how the usage models used in the POC could be adapted to your current business environment. This is also the point at which the POC team should develop a recommendation for further exploration of the capabilities, including an early adopter pilot.

Intel has developed a set of POC opportunities for corporations interested in investigating how Intel AMT could fit into their business. Contact your Intel account team or local sales office on how to get enrolled in POC evaluations.

Next steps

POC projects can give you a good sense of how a business may benefit from Intel AMT. The next step is to find out how your specific business environment could benefit from the new hardware-based capabilities. This is usually done through an early adopter pilot (described in the next discussion), with usage models tailored to suite your IT infrastructure and business needs.

Conduct an early adoption pilot

After the initial POC testing, you will know more about the value Intel AMT could bring to a business. To investigate these benefits in terms of your own network infrastructure, you should conduct an early adoption pilot.

An early adoption pilot is a limited deployment of PCs with Intel AMT, conducted with a select group of 15 or more users and with several trained IT technicians. It is usually conducted by an internal team, with help from service providers, third-party software vendors, and hardware suppliers. Planning usually involves business and engineering teams at a departmental level, and lasts three or four months. The pilot will probably require software upgrades to your management console.

Early adoption pilots are used to investigate and adapt known usage models – or create new models – for your specific environment. These modified usage models should be closely tied to your business processes and should include many users, so that you can effectively identify the benefits of deployment and the ROI for the business. The pilot can help you:

- Benchmark process improvements and costs reductions that would justify deployment of the new technology.
- Identify tasks that can be streamlined or automated using Intel AMT.
- Analyze the business value of the technology and set appropriate expectations for the return on investment of a broader production deployment of these PCs.
- Understand the setup and configuration process and the resource implications of a wide deployment of the technology. This includes realizing how to manage a mixed environment during the transition.
- Resolve any issues with management console ISVs.
- Train a staff and gain the skills necessary to use Intel AMT effectively before deploying the technology on a large scale.

Especially for a large enterprise with many systems to manage, an early adoption pilot can help you understand scalability, the setup and configuration process, and security credential management for this advanced technology. Such evaluations minimize the risk to your business processes while you identify and resolve issues associated with deploying the new technology. This is a critical step before integrating Intel AMT into IT management processes and deploying it across an enterprise.

General steps for an early adoption pilot

An early adoption pilot is conducted in a business environment, not an isolated lab. Businesses must carefully plan for the piloted systems to coexist with other systems in the environment, and determine how the rest of the non-Intel AMT systems will be managed.

In general, you would follow these steps to plan and conduct an early adoption pilot project:

1. **Select the early adoption team.** Pick people who can represent specific types of users and who can relate to your modified usage models. These people should represent the business pain points and be able to act as the personas that reflect your business processes.
2. **Refine the models.** Refine the storyboard of usage models to reflect specific business issues. This is an important step in making the usage cases match your business reality.
3. **Develop the details.** Develop detailed use cases and test cases to investigate the usage models and produce appropriate metrics to demonstrate the effectiveness of the capability being tested.
4. **Plan the build environment.** Develop a plan to add the new systems into the business environment without overly disrupting existing business processes.
5. **Plan for secure management processes.** Because an early adopter pilot is not conducted on an isolated network in a dedicated lab, you must plan realistic ways to manage security credentials and device setup and configuration. This may require working with your OEM and service provider to ensure the security is set up properly, and that the process can scale to your business needs.
6. **Test use cases and collect data.** Test use cases over a significant period of time, such as three or four months, in order to collect enough data to effectively evaluate the new technology.
7. **Analyze and summarize results.** Summarize the results, carefully evaluating them against expectations. This is not just about meeting ROI targets, but about providing a management experience acceptable to both IT technicians and end-users.

Next steps

Based on the results of the early adoption pilot, you may want to conduct another (or more) pilot project. These pilots could be used to investigate additional issues, address the needs of other departments, and evaluate more complex usage models. Or, you may feel ready to begin actual deployment of the technology to the production network, as described next.

Metrics for early adoption pilots

The metrics chosen for a technology evaluation should not be limited to technical measures, but should include business measures. This will help you better estimate the ROI of deploying the technology.

Security technologies

Refer the security section of this guide for information about security technologies, methods, and best practices for deploying this advanced technology.

Deployment recommendations

Based on the success of early adopter pilots, you may have a fairly good understanding of the potential ROI of a corporate-wide production deployment. You should now create a blueprint and schedule for a production roll-out of PCs with Intel AMT. This blueprint should include considerations such as funding for new equipment; updating, streamlining, and automating processes; training IT personnel; and getting back-end management consoles ready for the transition.

Production deployment usually takes several waves, in order to minimize disruptions to business. During deployment, keep these considerations in mind:

- Align deployment with system upgrade cycles.
- Make sure IT engineering and operation support teams are sufficiently trained as part of the upgrade cycle.
- Make sure there are consistent implementation and support processes for the usage models you are addressing. For example, make sure there are sufficient system-build, remote monitoring, problem-resolution, update, and upgrade processes available for the new PCs. This will help you gain the benefits of economy of scale.
- Continue to monitor and evaluate the effectiveness of and improvements in IT management processes. Using the same metrics from the early adoption pilot to do so after deployment can help consistently measure ROI and identify additional opportunities for improvement.

The primary advantage of Intel AMT is in gaining a high-performance, energy-efficient mainstream system that can be more easily managed from a remote service center. Deploying this technology in an enterprise environment can help IT achieve many goals, from reduced deskside visits, to improved remote diagnostics and repair, to increased security and compliance. By deploying PCs with Intel AMT in the production environment, corporations can see significantly lowered IT costs, increased user uptime, and less interruption to businesses.

Reaching the "last 10%"

When combined with third-party management software, Intel AMT allows IT technicians to access PCs that have traditionally been unavailable to the management console. For many businesses, the number of PCs unavailable at any given time can range from 5% to 20% or more.

Advantages of Intel AMT

Intel AMT capabilities can help IT organizations eliminate many deskside visits traditionally required for manual inventories; improve the speed and accuracy of remote diagnostics and repair; and significantly increase the speed and saturation of remote security updates.

[1] Source: Refer to the Intel white paper, "Reducing Costs with Intel Active Management Technology," 2005, Intel, for a detailed explanation of Intel's usage models and potential savings.

[2] Source: IT outsourcer evaluations of Intel vPro technology, as reported in various white papers, including: "Improving IT Services and Increasing User Uptime with Intel® vPro™ Technology," 2006, Intel; "Improving Asset Inventories and Reducing IT Costs with Intel® vPro™ Technology," 2006, Intel; and "Reducing Manual Processes with Improved Remote Security, Inventory, and Problem-Resolution," 2006, Intel. To read these and other industry evaluations of Intel vPro technology, visit the Intel Web site.

[3] Statements made by IT service providers reflect results of independent testing performed by those service providers in their own environment. Actual improvements in a production environment might vary. Other companies may see different results, depending on their IT service environment

Free ROI estimator

Intel provides a free ROI estimator on the Intel Web site to help you see how Intel AMT could benefit your enterprise environment.

Resources and training

To help you get started with deployment planning, Intel provides case studies, technology evaluations, and a return-on-investment (ROI) estimator on the Intel Web site. Intel can also provide businesses with personnel training for Intel AMT evaluations and early adopter pilot projects.

Case studies and technology evaluations

Intel has conducted many proof-of-concept pilots and studies, and has worked closely with industry-leading IT service providers to conduct extensive evaluations of Intel vPro technology, including Intel AMT. These evaluations have been conducted in lab settings, mock production environments, and actual customer environments.

Based on extensive analyses of the new capabilities of Intel AMT, Intel estimates an internal savings of $24M in IT costs once the technology is deployed throughout Intel's own organization.[1] Industry-leading IT service providers and customers have estimated similar benefits. For example, after evaluating the new capabilities many IT service providers expect to deploy PCs with Intel AMT to their corporate environments, with estimated benefits such as a 50% reduction in deskside visits for hardware problems, a 90% reduction in deskside visits required to resolve software problems, a 95% reduction in manual inventories, and a 95% improvement in the speed of security updates and patch deployment.[2, 3]

Case studies, evaluation reports, and white papers about these tests and customer deployments can be found on the Intel Web site.

ROI estimator available online

To help with business planning, Intel has provided a return-on-investment (ROI) estimator on the Intel Web site. The estimator can help IT administrators quantify the benefits of deploying Intel AMT in their business environment. Visit the Intel Web site to use the ROI estimator.

Training for Intel AMT

Deployment of PCs with Intel AMT requires system-administrator level knowledge of networking, system administration, and security methodologies. For less experienced system administrators, this guide provides background information on security methods and processes, requirements of various network environments, and configuration information.

Intel also offers training for proof-of-concept evaluations, early-adopter pilot projects, and BKM (best known methods) of deploying systems to an enterprise environment. Intel can also provide you with a list of authorized dealers and channel service providers who are experienced in deploying PCs with Intel AMT. For information about training, contact your Intel account team or local sales office.

For more information

Usage models and some typical use cases are described earlier in this guide. These use cases can help you identify processes where Intel AMT can offer improvements, and give you a starting point for building a POC evaluation or pilot study.

Case studies, evaluation reports, and white papers about POC tests and pilot studies in customer environments can be found on the Intel Web site. Contact your Intel account team or local sales office for help in setting up your own POC evaluation.

Intel® AMT

Intel® Active Management Technology (Intel® AMT) is one aspect of the new hardware-based capabilities of Intel® vPro™ technology

Appendix D
Glossary and Acronyms

This appendix lists glossary terms and acronyms commonly used in this guide.

Glossary

agent presence. Part of the Intel AMT system defense capabilities, agent presence provides a mechanism for third-party software applications (such as virus scan or antispyware) to register with Intel AMT and check in at regular intervals with hardware-based timers.

alerting. Intel AMT can send alerts to the remote management console regardless of PC power state or the state of the OS. IT administrators can subscribe or unsubscribe to specific alerts through the event manager service.

configuration service (CS). A third-party application that performs configuration services, such as loading networking information, Kerberos settings, access control lists, and other settings into Intel AMT.

configuration profile. The configuration profile contains the power policies for the Intel® Management Engine; and the Kerberos settings, access control lists, certificates and keys, and settings that activate the Intel AMT capabilities. See also local provisioning record (LPR).

configuration states. There are three setup and configuration states for PCs with Intel AMT: factory-default state, setup state, and configured state.

configured state. A fully configured state, in which Intel AMT has been configured with power policies, security settings and certificates, and the settings that activate Intel vPro technology capabilities. A PC whose Intel AMT capabilities have been configured, is ready to interact with management applications.

console redirection (SOL). Console redirection allows an authorized IT technician to remotely control a PC's keyboard and mouse through serial over LAN (SOL).

cyclical redundancy check (CRC). A mathematical method that permits errors in long runs of data to be detected with a very high degree of accuracy.

enterprise IT mode. An operational mode for large organizations that have a dedicated IT staff. This is an advanced networking mode that supports TLS and requires a setup application (the configuration service). Enterprise setup is the recommended networking mode.

event log. An Intel AMT event log, stored in nonvolatile memory. The event log is accessible even if the PC is powered down, the OS becomes inoperative, management agents are missing, or hardware (such as a hard drive) has failed.

factory-default state. A state in which initial security credentials have not been established for AMT capabilities. Intel AMT has the factory-defined settings. Typically this means that Intel AMT is enabled, networking is set to enterprise mode, TLS is enabled, and DHCP is enabled.

host. The PC's operating system. In static IP networking, the host has a different MAC address than the manageability MAC address used for the Intel Management Engine (which includes Intel AMT).

LPR. See local provisioning record.

local provisioning record (LPR). The local provisioning record is the file containing the information required to establish the initial, bootstrap networking and TLS security credentials for Intel AMT. This information consists of administrator password, provisioning passphrase (PPS), and provisioning ID (PID). The LPR is used to load security credentials into Intel AMT during setup via a USB-key storage device. Because the USB-key setup procedure is an automated procedure, the LPR is transparent to the IT administrator setting up the PCs. LPR files are not used in the manual setup procedure. In the manual setup procedure, the initial security credentials (password, PPS, and PID) for Intel AMT are entered manually, one at a time via the MEBx. *See also* configuration profile.**)**

management device. A system (not the PC with Intel AMT being deployed) used to perform setup and/or configuration for the PC with Intel AMT.

MEBx. The Intel Management Engine BIOS extension. The MEBx settings that are available to IT administrators, and the default values of those settings are vendor-dependent.

network outbreak containment (NOC). Part of the Intel AMT system defense capabilities, NOC provides hardware-based filters for inbound and outbound network traffic, port isolation based on IT-defined policies, and the ability to rate-limit network traffic to allow more time to investigate a threat.

networking mode. See operational mode.

networking type. PCs with Intel AMT can be set up for two types of networking: dynamic IP or static IP. Both types of networking are supported by enterprise mode and small-business mode.

nonvolatile memory. A persistent, tamper-resistant space divided into three segments: storage for the signed, encrypted Intel Management Engine and the information used by Intel AMT; storage for hardware asset information, BIOS configuration information, UUID, event log, and other system information; and storage (the 3PDS) configurable by authorized IT administrators for use by third-party software.

operational mode. Intel AMT can be set up for two types of operational networking (also called networking models): enterprise mode and small-business mode. Both modes support dynamic and static IP networking. The PC manufacturer typically specifies the default networking type when building the Intel vPro technology flash image.

PC. A PC with Intel AMT.

remote boot/redirected boot. A hardware-based capability that allows authorized technicians to remotely boot a PC to a clean state, or redirect the boot device for a problem PC to a clean image on local storage, a CD at the help desk, an image on a remediation server, or to some other remote device. Remote boot is provided through integrated drive electronics redirect (IDE-R).

remote power-up. A hardware-based capability that allows authorized technicians to power up, power down, power cycle, or reset PCs from the management console.

Intel AMT states
Intel AMT has three states: factory-default state, setup state (initial security credentials loaded), and configured state (operational state).

setup state. A state in which the initial, bootstrap security credentials have been established for Intel AMT: initial administrator password, provisioning passphrase (the PPS, or preshared key), and provisioning identifier (PID). When Intel AMT has been set up, it is ready to receive enterprise configuration settings from a configuration service.

small-business mode. A simplified networking mode that does not support TLS, does not require a setup application, and does not require DHCP or DNS.

simple object access protocol (SOAP). A protocol that allows IT administrators to communicate with PC hardware across the network.

third-party data store (3PDS). A persistent space in the Intel AMT nonvolatile memory where third-party vendors can store information, such as software version numbers, .DAT file information, machine IDs, pointers to database information, or other data.

universal unique identifier (UUID). The UUID is the universally unique identifier for the Intel AMT system, as defined by RFC 2459; section 4.1.2.8. The UUID is stored in the Intel AMT persistent, nonvolatile memory in each PC, and is protected by HTTP digest authentication, TLS, and access control lists.

Acronyms

3PDS	Third-party data store
ACL	Access control list
AD	Microsoft Active Directory
AES	Advanced encryption standard
AMT	Intel® Active Management Technology (Intel® AMT)
API	Application programming interface
BIOS	Basic input/output system
BKM	Best known methods
CA	Certificate authority
CRC	cyclical redundancy check.
CRL	Certificate revocation list(s)
CS	configuration service
DHCP	Dynamic host configuration protocol
DN	Domain name
DNS	Domain name server
EACL	Enterprise access control list
FPACL	Factory-partner access control list
FQDN	Fully qualified domain name
FWSK	Firmware signing key(s)
GUI	Graphical user interface
HECI	Host embedded controller interface
HTTP	HyperText transfer protocol
ICH	I/O controller hub
ID	Identifier
IDE-R	Integrated device electronics redirect. *See glossary entry for* remote boot.
IETF	Internet engineering task force
IP	Internet protocol
ISV	Independent software vendor, a third-party software vendor
IT	Information technology

IDE-R
The remote-boot capability allows remote boot of a PC from its own boot device, or redirected boot of the OS to a remote boot device, such as a remediation server or an image on network share.

POCs
Proof-of-concept evaluations and pilot tests are described in the deployment-planning appendix.

KDC	Key distribution center
LAN	Local area network
LPR	Local provision record
MAC	Media access controller
ME	Management engine
MEBx	Management engine BIOS extension
MEI	Management engine interface
NOC	Network outbreak containment
OEM	Original equipment manufacturer
OS	Operating system
PC	A PC with Intel AMT
PET	Platform event trap
PID	Provisioning identifier
PKI	Preshared-key infrastructure
PMS	Premaster secret
POC	Proof of concept
POST	Power-on self-test
PPS	Provisioning pass-phrase
PRNG	Pseudo-random number generator
PSK	Preshared key
PXE	Preexecution boot environment. *See glossary entry for* remote boot.
RFC	Request for comments (Internet).
RNG	Random-number generator
ROM	Read-only memory
RSA	An acronym comprised of the initials of the last names of the founders of this security method.
SCA	Setup and configuration application
SCS	Intel® Active Management Technology Setup and Configuration Service Product
SDK	Software development kit
SMB	Small- or medium-business
SNMP	Simple network management protocol

SOL

Console redirection allows a technician to remotely control and guide a PC through a troubleshooting session, firmware update, or other remote task, minimizing the traditional need for user participation or intervention.

SOAP	Simple object access protocol
SOL	Serial over LAN. *See glossary entry for* console redirection.
SSL	Secure sockets layer
SX	Sleep state 1 through 5. (Note that S0 is the fully operational state.)
TCL	Tool control language
TCO	Total cost of ownership
TCP/IP	Transmission control protocol/internet protocol
TLS	Transport layer security
TLS CA	Transport layer security certificate authority
UI	Unique identifier
UI	User interface
USB	Universal serial bus
UUID	Universally unique identifier. *See glossary entry for* UUID
VLAN	Virtual local area network
VT	Intel® Virtualization Technology (Intel® VT)
WOL	Wake on LAN. *See glossary entry for* remote boot
WSDL	Web services description language

Index